(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 October 2018 (04.10.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/183572 A1

(51) International Patent Classification:
H03M 13/00 (2006.01)

(21) International Application Number:
PCT/US2018/024952

(22) International Filing Date:
28 March 2018 (28.03.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/478,130 29 March 2017 (29.03.2017) US
62/478,117 29 March 2017 (29.03.2017) US

(71) Applicant: **BOARD OF REGENTS, THE UNIVERSITY OF TEXAS SYSTEM** [US/US]; 210 West 7th Street, Austin, TX 78701 (US).

(72) Inventors: **ORSHANSKY, Michael**; The University of Texas at Austin, 2501 Speedway, C0803, Austin, TX 78712 (US). **WANG, Ye**; The University of Texis at Austin, 2501 Speedway, C0803, Austin, TX 78712 (US).

(74) Agent: **VOIGT, Robert, A., Jr.**; Winstead, P.C., P.O. Box 131851, Dallas, TX 75313 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) **Title:** REDUCING AMOUNT OF HELPER DATA IN SILICON PHYSICAL UNCLONABLE FUNCTIONS VIA LOSSY COMPRESSION WITHOUT PRODUCTION-TIME ERROR CHARACTERIZATION

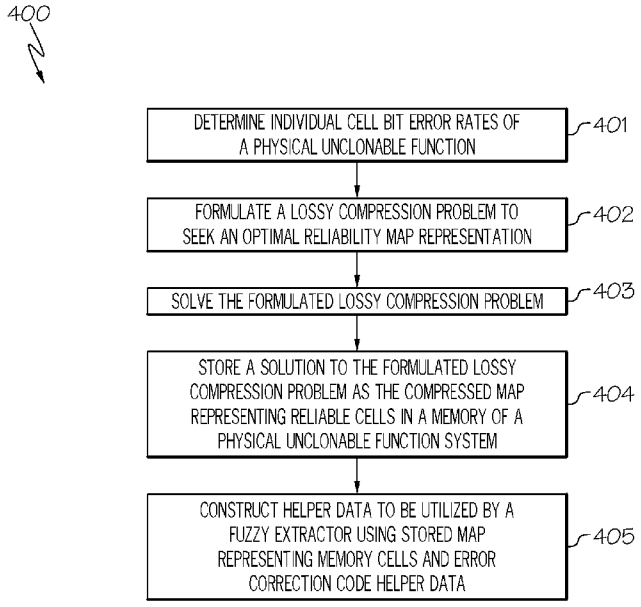


FIG. 4

(57) **Abstract:** A method, system and computer program product for reducing the amount of helper data that needs to be stored using two innovative techniques. The first technique uses bit-error-rate (BER)-aware lossy compression. By treating a fraction of reliable bits as unreliable, it effectively reduces the size of the reliability mask. With the view of practical costs of production-time error characterization, the second technique enables economically feasible across-temperature per-bit BER evaluation for use in a number of fuzzy extractor optimizations based on bit-selection to reduce overall BER (with or without subsequent compression) using room-temperature only production-time characterization. The technique is based on stochastic concentration theory and allows efficiently forming confidence intervals for average across- temperature BER of a selected set of bits. By using these techniques, it is economically

[Continued on next page]

WO 2018/183572 A1

SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

feasible to achieve a dramatic reduction in the amount of helper data that needs to be stored in non-volatile memory and/or one-time-programmable memory.

REDUCING AMOUNT OF HELPER DATA IN SILICON PHYSICAL UNCLONABLE FUNCTIONS VIA LOSSY COMPRESSION WITHOUT PRODUCTION-TIME ERROR CHARACTERIZATION

TECHNICAL FIELD

[0001] The present invention relates generally to physical unclonable functions, and more particularly to reducing the amount of helper data in silicon physical unclonable functions via lossy compression without production-time error characterization.

BACKGROUND

[0002] In cryptography, a physical unclonable function ("PUF") is a physical entity that is embodied in a physical structure and is easy to evaluate but hard to predict. Such PUFs may be easy to make but practically impossible to duplicate, even given the exact manufacturing process that produced it.

[0003] PUFs depend on the uniqueness of their physical microstructure. This microstructure depends on random physical factors introduced during manufacturing. These factors are unpredictable and uncontrollable which makes it virtually impossible to duplicate or clone the structure.

[0004] Rather than embodying a single cryptographic key, PUFs implement challenge–response authentication to evaluate this microstructure. When a physical stimulus is applied to the structure, it reacts in an unpredictable (but repeatable) way due to the complex interaction of the stimulus with the physical microstructure of the device. This exact microstructure depends on physical factors introduced during manufacture which are unpredictable (like a fair coin). The applied stimulus is called the challenge, and the reaction of the PUF is called the response. A specific challenge and its corresponding response together form a challenge–response pair ("CRP"). The device's identity is established by the properties of the microstructure itself. As this structure is not directly revealed by the challenge-response mechanism, such a device is resistant to spoofing attacks. In some PUFs, such as "weak PUFs," the challenge is a simple act of powering up a circuit.

[0005] The key distinction among different PUF constructions is between strong and weak PUFs, based on the rate at which the number of CRPs grows with the size of physical realization

of a PUF. Weak PUFs are characterized by a small number of CRPs while strong PUFs are systems with a large number or even exponential number of CRPs.

[0006] Silicon physical unclonable functions (PUFs) are widely used in emerging hardware security applications, such as device identification, authentication, and cryptographic key generation. As discussed above, PUFs generate unique randomness by exploiting inherent random process variation during fabrication. Among them, Static Random-Access Memory (SRAM) PUFs that produce unique signatures with power-up states are appealing because SRAMs are widely available standard components in a multitude of existing integrated circuits (ICs).

[0007] However, the major challenge of utilizing silicon PUFs, including SRAM PUFs, lies in the reliability of responses. Ideally, an SRAM PUF bit produces a unique and identical power-up value under each evaluation. In fact, power-up is a cell-specific stochastic process determined jointly by device mismatch, instantaneous noise, and environment variation.

[0008] The standard method to ensure PUF reliability in the key derivation context is to use a fuzzy extractor that utilizes an error correction code (ECC). A fuzzy extractor algorithm involves two phases: enrollment and reconstruction. During enrollment, an ECC is used to encode raw PUF responses and compute the code syndrome to be used as helper data for reconstruction. The helper data is assumed to be public and is stored in non-volatile memory.

[0009] In some applications of PUF-based key generation for original silicon manufacturers, one-time-programmable (OTP) memory (e.g., fuses) is preferred as it cannot be modified by an adversary. In these settings, the helper data needs to be stored on-die, prior to the package-level or board-level resources (e.g., high-capacity Flash memory) are available. However, in many platforms, e.g., field-programmable gate arrays (FPGAs), the amount of OTP memory available is severely limited. As a result, the amount of required helper data should be reduced.

SUMMARY

[0010] In one embodiment of the present invention, a method for reducing the amount of helper data that needs to be stored comprises determining individual cell bit-error-rates of a physical unclonable function. The method further comprises formulating a lossy compression problem using the determined individual cell bit-error-rates of the physical unclonable function. The method additionally comprises solving the formulated lossy compression problem. Furthermore, the method comprises storing a solution to the formulated lossy compression problem as a map representing reliable cells in a memory of a physical unclonable function system. Additionally, the method comprises constructing helper data to be utilized by a fuzzy extractor using the map representing reliable cells and error correction code helper data.

[0011] Other forms of the embodiment of the method described above are in a system and in a computer program product.

[0012] In another embodiment of the present invention, a method for reducing the amount of helper data that needs to be stored comprises extracting distribution of cells' across-temperature bit-error-rates using a population-based analysis at a technology development phase. The method further comprises measuring only nominal one-probabilities for each cell at a production phase. The method additionally comprises using the population-based analysis of the cells' across-temperature bit-error-rates for the measured nominal one-probabilities for each cell to derive a confidence level for an average across-temperature bit-error-rate of a set of cells. Furthermore, the method comprises optimizing a fuzzy extractor by identifying a subset of more reliable bits out of a population of physical unclonable function bits using the derived confidence level for the average across-temperature bit-error-rate of the set of cells.

[0013] Other forms of the embodiment of the method described above are in a system and in a computer program product.

[0014] In a further embodiment of the present invention, a method for helper data size reduction for strong physical unclonable functions comprises generating pseudo random numbers. The method further comprises inputting the generated pseudo random numbers to a strong physical unclonable function which outputs a set of responses to the inputted pseudo random numbers as input challenges that are stored in a one-dimensional indexed array. The method additionally comprises applying compression and confidence interval estimation techniques to form a

compact representation of challenge response pairs of the strong physical unclonable function as entries of the array. Furthermore, the method comprises storing the representation as reduced helper data in a memory of a physical unclonable function system.

[0015] Other forms of the embodiment of the method described above are in a system and in a computer program product.

[0016] The foregoing has outlined rather generally the features and technical advantages of one or more embodiments of the present invention in order that the detailed description of the present invention that follows may be better understood. Additional features and advantages of the present invention will be described hereinafter which may form the subject of the claims of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] A better understanding of the present invention can be obtained when the following detailed description is considered in conjunction with the following drawings, in which:

[0018] Figure 1 illustrates an exemplary PUF system in accordance with an embodiment of the present invention;

[0019] Figure 2 shows a conventional PUF-based key generation flow in accordance with an embodiment of the present invention;

[0020] Figure 3 illustrates a hardware configuration of a computing device which is representative of a hardware environment for practicing the present invention; and

[0021] Figure 4 is a flowchart of a method for reducing the helper data size by treating a certain fraction of reliable bits as being unreliable in accordance with an embodiment of the present invention;

[0022] Figure 5 is a flowchart of a method for bit-specific across-temperature BER characterization that enables HDS reduction and other fuzzy extractor optimizations in accordance with an embodiment of the present invention;

[0023] Figure 6 is a graph depicting individual cell's maximum across-temperature BERs plotted against nominal-temperature one-probabilities in accordance with an embodiment of the present invention; and

[0024] Figure 7 is a flowchart of a method for helper data size reduction for strong PUFs in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

[0025] As discussed in the Background section, the standard method to ensure PUF reliability in the key derivation context is to use a fuzzy extractor that utilizes an error correction code. A fuzzy extractor algorithm involves two phases: enrollment and reconstruction. During enrollment, an ECC is used to encode raw PUF responses and compute the code syndrome or code offset to be used as helper data for reconstruction. The helper data is assumed to be public and is stored in non-volatile memory. For key generation applications for original semiconductor manufacturers, helper data needs to be stored on the silicon die, prior to the package-level and/or board-level resources becoming available. Thus, for original semiconductor companies, one-time-programmable (OTP) memory (e.g., fuses) is preferred. An additional advantage of OTP is that it cannot be easily modified by an adversary. However, in many platforms, e.g., FPGAs, the amount of OTP memory available is severely limited. As a result, the amount of required helper data should be reduced.

[0026] The present invention allows a significant reduction of helper data size (HDS) through two innovative techniques. The first technique uses bit-error-rate (BER)-aware lossy compression by treating a fraction of the reliable bits as unreliable thereby effectively reducing the size of the map needed to represent these bits. With the view of practical costs of production-time error characterization, the second technique enables economically feasible across-temperature per-bit BER evaluation for use in a number of fuzzy extractor optimizations based on bit-selection to reduce overall BER (with or without subsequent compression) using room-temperature only production-time characterization. The method is based on stochastic concentration theory and allows efficient formation of confidence intervals for true average worst-case BER of a selected set of bits.

[0027] As discussed below in greater detail, the present invention proposes two innovative techniques based on lossy compression to reduce the total HDS dramatically and optimality. The first technique of lossy compression involves sacrificing a certain fraction of reliable bits by treating them as unreliable thereby leading to effective compression and large HDS reduction. In one embodiment, the present invention minimizes HDS when complete bit-specific error information is available across a range of operating conditions. To achieve that, a two-phase joint BER minimization and reliability mask compression algorithm is developed. A derived

codebook is used to select a better solution that minimizes the overall average error of selected bits. This is done via the formulation using an integer linear programming problem (ILP). By utilizing the Lagrangian relaxation heuristics, the proposed ILP formulation can be decomposed into small separable sub-problems with efficient greedy-based linear-time solutions. Moreover, the proposed lossy compression algorithm does not leak any information about the key material.

[0028] The benefits of the technique are significant. Consider deriving a 128-bit key with a failure rate of 10^{-6} from the SRAM cells with an average BER of 10.22%. A direct implementation of fuzzy extractor requires 1060 raw source bits and 932 OTP bits for helper data. A bit-selection scheme with lossless compression reduces the helper data to 288 bits. After the proposed lossy compression, only 206 bits of HDS are needed, which is a 25% reduction, though at the cost of doubling the number of raw bits.

[0029] However, the approach above requires a possibly expensive BER characterization effort in which the reliability information under all possible conditions for each bit of each production PUF chip is extracted. Worst-case BER characterization across all working conditions may be unacceptably costly in a production environment.

[0030] The second technique practically enables multiple fuzzy extractor optimization strategies, which include lossy compression as described, other lossy compression strategies, lossless compression, or no compression methods (e.g., dark bit masking) that operate by identifying a subset of more reliable bits out of a population of all PUF bits. The second technique allows economically feasible across-temperature BER characterization operation via a construction of a tight confidence interval of the worst-case BER using multidimensional statistics. This is enabled by the observation that across-temperature (worst-case) BERs are correlated with their nominal-temperature one-probabilities for stable cells. The present invention performs a one-time large sample characterization experiment, predicts the average worst-case BERs based on nominal one-probabilities, and allows fuzzy extractor optimization strategies using the obtained confidence interval of the average worst-case BER for selected cells. By utilizing a stochastic concentration inequality, it is shown that for SRAM cells with sufficient size, the true average worst-case BER can be accurately estimated. The accuracy of estimation enables the guarantee of key reconstruction with overwhelmingly high probability.

[0031] The result is dramatic: compared to the maskless alternative, the method of the present invention still results in an overall 2.3X helper data reduction for extracting a 128-bit key and a 3X reduction for a 256-bit key, while allowing key reconstruction to fail in only 10^{-5} cases.

[0032] Referring now to the Figures in detail, Figure 1 illustrates an exemplary PUF system 100 in accordance with an embodiment of the present invention. PUF system 100 includes a Static Random-Access Memory (SRAM) PUF 101, which refers to SRAM being a source of PUF bits.

[0033] PUF system 100 further includes a reading circuit 102 for reading the contents from SRAM PUF 101.

[0034] Furthermore, PUF system 100 includes a PUF control logic 103 connected to reading circuit 102. PUF control logic 103 may be implemented in hardware on an integrated circuit. PUF control logic 103 may comprise a data processor (e.g., a central processing unit) for executing a software program to obtain the functionality of PUF control logic 103.

[0035] Additionally, PUF system 100 includes a memory 104 connected to PUF control logic 103. In one embodiment, memory 104 is non-volatile, writable memory, such as a flash memory, EPROM memory, EEPROM, e-fuses, etc. In one embodiment, memory 104 is a one-time-programmable (OTP) memory. In one embodiment, memory 104 stores helper data (further discussion of helper data provided below). In one embodiment, memory 104 stores a program for reducing the amount of helper data that needs to be stored as discussed below in connection with Figures 4-6. The instructions of this program may be executed by the data processor of PUF control logic 103. In one embodiment, memory 104 also stores helper data for PUF reconstruction.

[0036] In one embodiment, the program for reducing the amount of helper data that needs to be stored, as discussed below in connection with Figures 4-6, is executed by a processor of a computing device. A description of an embodiment of the hardware configuration of such a computing device is provided further below in connection with Figure 3.

[0037] In one embodiment, PUF control logic 103 is configured to receive the PUF data read by reading circuit 102 and to receive helper data from memory 104. Using a helper data algorithm (also referred to as a fuzzy extractor), which may be executed on PUF control logic 103, the PUF

data obtained is processed using the helper data. As a result of this processing, the variation which may be present in the PUF data, is removed.

[0038] An explanation of using SRAM PUF 101 to create a cryptographic key involving the enrollment and reconstruction phases is discussed further below in connection with Figure 2.

[0039] Figure 1 is not to be limited in scope to the depicted elements. For example, PUF system 100 is not to be limited to using an SRAM PUF. Other PUFs could be used.

[0040] A discussion regarding the PUF-based key generation algorithm based on the fuzzy extractor (consists of two phases: enrollment and reconstruction) is now deemed appropriate.

[0041] Referring to the BER modeling and characterization, cell i is defined with the one-probabilty $p_i(T, Vdd)$ as the probability of returning a 1 from one random power up under temperature T and supply voltage Vdd. The enrollment response X_i's are derived via majority voting under nominal voltage and temperature: $X_i = 1$ if $p_i(T_{ref}, Vdd_{ref}) > 0.5$ and $X_i = 0$ otherwise. BER $p_{ei}(T, Vdd)$ can be derived from one probability $p_i(T, Vdd)$ and enrollment response X_i accordingly: $p_{ei}(T, Vdd) = p_i(T, Vdd)$ if $X_i = 0$ and $p_{ei}(T, Vdd) = 1 - p_i(T, Vdd)$ if $X_i = 1$. To guarantee key reconstruction under all possible environmental condition, one needs to ensure that even with the worst-case BERs p_{wi}, defined by $p_{wi} = \max_{T \in [T_{min}, T_{max}], V_{dd} \in [V_{min}, V_{max}]} p_{ei}(T, V_{dd})$, the key is reproduced reliably.

[0042] Referring to Figure 2, Figure 2 shows a conventional PUF-based key generation flow in accordance with an embodiment of the present invention. A fuzzy extractor consists of two phases: enrollment 201 and reconstruction 202. The following discussion of the present invention uses the linear code and syndrome-based fuzzy extractor for enrollment and reconstruction but the present invention can also be extended to using the code-offset-based fuzzy extractor or even non-linear codes. It is noted that in the discussion below, vectors and matrices are denoted with bold symbols with dimension on superscript, which can be dropped for convenience in case of no confusion. In the enrollment phase, noisy raw PUF responses X are fed into an encoder 203 for a code $C(n,k,t)$ with length n, dimension k, error-correcting capacity t

and parity-check matrix H to extract the syndrome $W = XH^T$ that is later used as helper data (stored in helper data storage 204) in reconstruction. Reconstruction phase 202 takes another PUF measurement X^1 and the previous helper data W as input, and calculates the XORed syndrome $S = X^1H^T \oplus W$. Due to linearity of codes, $S = (X \oplus X^1)H^T$. If the Hamming distance $HD(X,X^1) = HW(X \oplus X^1)$ is no larger than the error-correcting capacity t, X^1 can be decoded by decoder 205 to restore X. The code syndrome with length $(n-k)$ needs to be stored in non-volatile memory, such as one-time-programmable (OTP) memory (e.g., memory 104).

[0043] Typical cryptographic applications pose security requirements on X in terms of conditional min-entropy $H_\infty(X|W)$. Introduction of helper data inevitably discloses partial information on the source bits X, and the left-over entropy of X conditioned on W is given by:

$$H_\infty(X|W) \geq H_\infty(X) - (n - k).$$

[0044] The practical overhead of implementing fuzzy extractors depends on the choice of an error correction code which is largely determined by PUF noise level. For a given security level and reconstruction failure probability, helper data length of code syndrome scales quickly with the increase of the bit-error-rate (BER). For n bit responses with uniform BER p_e, the Hamming distance $HD(X,X^1)$ follows a binomial distribution $B(n,p_e)$. Therefore, the failure rate P_{Fail} of reconstruction is

$$\begin{aligned} P_{\text{Fail}} &= 1 - F(t; n, p_e) \\ &= \sum_{i=t+1}^{n} \binom{n}{i} p_e^i (1-p_e)^{(n-i)}, \end{aligned}$$

where $F(t;n,p_e)$ denotes the corresponding cumulative distribution function (CDF) of $B(n,p_e)$. For PUF responses with heterogeneous BERs $(p_{e1},p_{e2},...,p_{en})$, Hamming distance $HD(X,X^1)$ follows Poisson binomial distribution. In one embodiment, the present invention uses a binomial distribution with p_e as the average $p_e = \sum_{i=1}^{n} p_{ei}/n$ as an approximation of the corresponding Poisson binomial distribution.

[0045] For ECCs with fixed block length n, there is a fundamental trade-off between dimension k and the error correction capacity t. Many SRAM PUF designs utilize concatenated codes with repetition codes as inner code and (shortened) BCH codes as outer code in the implementation of

the fuzzy extractor. Concatenated codes are typically more efficient than single codes in terms of code length and HDS.

[0046] As discussed above, the program for reducing the amount of helper data that needs to be stored as discussed below in connection with Figures 4-7 is executed by a processor of a computing device. A description of an embodiment of the hardware configuration of such a computing device is provided below in connection with Figure 3.

[0047] Referring now to Figure 3, Figure 3 illustrates a hardware configuration of computing device 300 which is representative of a hardware environment for practicing the present invention. Referring to Figure 3, computing device 300 has a processor 301 coupled to various other components by system bus 302. An operating system 303 runs on processor 301 and provides control and coordinates the functions of the various components of Figure 3. An application 304 in accordance with the principles of the present invention runs in conjunction with operating system 303 and provides calls to operating system 303 where the calls implement the various functions or services to be performed by application 304. Application 304 may include, for example, a program for reducing the amount of helper data that needs to be stored as discussed further below in connection with Figures 4-6.

[0048] Referring again to Figure 3, read-only memory ("ROM") 305 is coupled to system bus 302 and includes a basic input/output system ("BIOS") that controls certain basic functions of computing device 300. Random access memory ("RAM") 306 and disk adapter 307 are also coupled to system bus 302. It should be noted that software components including operating system 303 and application 304 may be loaded into RAM 306, which may be computing device's 300 main memory for execution. Disk adapter 307 may be an integrated drive electronics ("IDE") adapter that communicates with a disk unit 308, e.g., disk drive.

[0049] Computing device 300 may further include a communications adapter 309 coupled to bus 302. Communications adapter 309 interconnects bus 302 with an outside network thereby enabling computing device 300 to communicate with other devices.

[0050] Computing device 300 of Figure 3 is not to be limited in scope to the elements depicted in Figure 3 and may include fewer or additional elements than depicted in Figure 3.

[0051] The present invention may be a system, a method, and/or a computer program product. The computer program product may include a computer readable storage medium (or media) having computer readable program instructions thereon for causing a processor to carry out aspects of the present invention.

[0052] The computer readable storage medium can be a tangible device that can retain and store instructions for use by an instruction execution device. The computer readable storage medium may be, for example, but is not limited to, an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, or any suitable combination of the foregoing. A non-exhaustive list of more specific examples of the computer readable storage medium includes the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a static random access memory (SRAM), a portable compact disc read-only memory (CD-ROM), a digital versatile disk (DVD), a memory stick, a floppy disk, a mechanically encoded device such as punch-cards or raised structures in a groove having instructions recorded thereon, and any suitable combination of the foregoing. A computer readable storage medium, as used herein, is not to be construed as being transitory signals *per se*, such as radio waves or other freely propagating electromagnetic waves, electromagnetic waves propagating through a waveguide or other transmission media (e.g., light pulses passing through a fiber-optic cable), or electrical signals transmitted through a wire.

[0053] Computer readable program instructions described herein can be downloaded to respective computing/processing devices from a computer readable storage medium or to an external computer or external storage device via a network, for example, the Internet, a local area network, a wide area network and/or a wireless network. The network may comprise copper transmission cables, optical transmission fibers, wireless transmission, routers, firewalls, switches, gateway computers and/or edge servers. A network adapter card or network interface in each computing/processing device receives computer readable program instructions from the network and forwards the computer readable program instructions for storage in a computer readable storage medium within the respective computing/processing device.

[0054] Computer readable program instructions for carrying out operations of the present invention may be assembler instructions, instruction-set-architecture (ISA) instructions, machine

instructions, machine dependent instructions, microcode, firmware instructions, state-setting data, or either source code or object code written in any combination of one or more programming languages, including an object oriented programming language such as Smalltalk, C++ or the like, and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The computer readable program instructions may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some embodiments, electronic circuitry including, for example, programmable logic circuitry, field-programmable gate arrays (FPGA), or programmable logic arrays (PLA) may execute the computer readable program instructions by utilizing state information of the computer readable program instructions to personalize the electronic circuitry, in order to perform aspects of the present invention.

[0055] Aspects of the present invention are described herein with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer readable program instructions.

[0056] These computer readable program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks. These computer readable program instructions may also be stored in a computer readable storage medium that can direct a computer, a programmable data processing apparatus, and/or other devices to function in a particular manner, such that the computer readable storage medium having instructions stored therein comprises an article of manufacture including instructions which

implement aspects of the function/act specified in the flowchart and/or block diagram block or blocks.

[0057] The computer readable program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other device to cause a series of operational steps to be performed on the computer, other programmable apparatus or other device to produce a computer implemented process, such that the instructions which execute on the computer, other programmable apparatus, or other device implement the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0058] The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods, and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of instructions, which comprises one or more executable instructions for implementing the specified logical function(s). In some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts or carry out combinations of special purpose hardware and computer instructions.

[0059] The principles of the present invention provide a means for reducing the helper data size as discussed below in connection with Figures 4-7. Figure 4 is a flowchart of a method for reducing the helper data size by treating a certain fraction of reliable bits as being unreliable. Figure 5 is a flowchart of a method for bit-specific across-temperature BER characterization that enables HDS reduction and other fuzzy extractor optimizations. Figure 6 is a graph depicting individual cell's maximum across-temperature BERs plotted against nominal-temperature one-probabilities. Figure 7 is a flowchart of a method for reducing the helper data size for strong PUFs.

[0060] As stated above, Figure 4 is a flowchart of a method 400 for reducing the helper data size by treating a certain fraction of reliable bits as being unreliable in accordance with an embodiment of the present invention.

[0061] Method 400 is a method corresponding to the present invention's joint HDS reduction and BER minimization algorithm referred above. The essential idea is a lossy compression: extra reliable bits can be traded for reduced HDS on reliability masks.

[0062] Referring to Figure 4, in conjunction with Figures 1-3, in step 401, the individual cell bit-error-rates of a physical unclonable function (PUF) is determined.

[0063] In step 402, a lossy compression problem is formulated to seek an optimal reliability map representation. An example of such a lossy compression problem is an integer linear programming (ILP) problem. In one embodiment, the lossy compression problem is formulated using the determined individual cell bit-error-rates of the PUF to seek an optimal mask representation. While the following discusses a formulation based on ILP and/or the solution based on generating a codebook (e.g., randomized codebook), such as based on a rate of compression and determined cell-specific BERs, the present invention is not to be limited in scope to such embodiments. Instead, the present invention may utilize other lossy compression problem formulations.

[0064] In one embodiment, the ILP seeks an optimal mapping from SRAM segments into codewords in the generated codebook. The ILP problem seeks to minimize the average worst-case error rate of selected SRAM cells under the constraint of a sufficient number of "reliable" bits retained by the ILP problem. "Reliable bits," as used herein, refer to the bits that are retained by the compression algorithm for use in the fuzzy extractor as opposed to the low-reliability bits.

[0065] In step 403, the formulated lossy compression problem is solved. For example, a Lagrangian relaxation method is used for solving the integer linear programming problem to further reduce the number of bits storing helper data in a memory of a PUF system.

[0066] In step 404, a solution to the formulated lossy compression problem as the compressed map representing reliable cells is stored in a memory (e.g., memory 104) of the PUF system (e.g., PUF system 100).

[0067] In step 405, helper data to be utilized by the fuzzy extractor is constructed using the stored map and the error correction code helper data.

[0068] A more detailed discussion regarding method 400 is provided below in connection with the discussion of Algorithm 1.

[0069] The algorithm of the present invention, shown below in Algorithm 1, proceeds by partitioning a sequence of SRAM cells with size n into k segments, each of length $l = n/k$. It consists of two phases: (1) a codebook construction step enabling compact expression of reliability masks, and (2) an error minimization step that maps the reliability mask of each segment of SRAM cells to one codeword from the codebook.

[0070] The lossy compression algorithm defines a lossy ratio D ($0 < D < 1$) as the target ratio of further discarded reliable bits. For example, $C = 0.5$ and $D = 0.5$ means that 50% raw bits are considered reliable and among all reliable bits 50% of them are discarded, namely, 25% of the original raw bits are finally utilized.

[0071] The codebook C is designed to contains an all-zero vector $\mathbf{O}^l$ and $(2^{lR(D)} - 1)$ random sampled vectors of length l, in which $R(D)$ is defined as:

$$R(D) = H(C) - (1 - C + CD)H\left(\frac{1 - C}{1 - C + CD}\right).$$

$lR(D)$ bits are able to represent a codeword via indexing since the codebook C has the cardinality of $|C| = 2^{lRD}$. Therefore, significant reduction of HDS for reliability mask requires that $R(D) \ll 1$. Each coordinate $C[j]_k$ of each non-zero codeword $C[j]$ follows an i.i.d. binary distribution that

$$\Pr(C[j]_k = 0) = 1 - C + CD$$

[0072] Similar to masks constructed via the dark-bit masking, a "1" in a codeword means that the corresponding SRAM cell is masked as reliable and selected for the key generation.

[0073] Algorithm 1:

Algorithm 1 Lossy compression for HDS reduction

```
procedure LossyCompress(p_w, M, n, N, l, C, D)
    Sample codebook C;
    L ← 0, R ← 1, n_λ ← 0;
    while (n_λ ≠ n) do
        λ ← (L + R)/2;
        n_λ ← 0
        for (i = 1; i ≤ N/l; i++) do
            for (j = 1; j = 2^HW(D); j++) do
                S_ij = Σ_{k=1}^{l} p_{w,ik} C[j]_k;
            end for
            j* = arg min_j((S_ij − λ HW(C[j])));
            M[i] ← C[j*];
            n_λ ← n_λ + HW(C[j*]);
        end for
        if (n_λ < n) then
            L ← λ;
        end if
        if (n_λ > n) then
            R ← λ;
        end if
    end while
end procedure
```

[0074] After the codebook construction, the second phase takes individual BERs as input and pursues an optimal mapping of reliability masks for each segment of SRAM cells, in order to achieve the overall BER minimization. The binary decision variables x_{ij}'s, $\forall i \in |\mathbf{M}|, j \in |\mathbf{C}|$ are defined to indicate the encoding of the mask $\mathbf{M}[i]$ from the i-th segment of SRAM cells:

$$x_{ij} = 1, \text{ iff } \mathrm{Enc}(M[i]) = C[j].$$

[0075] As previously mentioned, encoding $\mathbf{M}[i]$ with a j-th codeword $C[j]$ provides HW($C[j]$) reliable output bits with the corresponding sum of BERs S_{ij} as

$$S_{ij} = \sum_{k=1}^{l} p_{w,ik} C[j]_k,$$

in which $p_{w,ik}$ denotes the worst-case BER of the k-th source bit in the i-th segment $\mathbf{M}[i]$.

[0076] The optimization seeking the optimal effective BER under the constraint of a sufficient number of reliable output bits is formulated as an integer linear programming problem:

$$\begin{aligned} \min_{x_{ij}} \quad & \sum_{i,j} S_{ij} x_{ij} \\ \text{s.t.} \quad & \sum_{i,j} \mathrm{HW}(C[j]) x_{ij} \geq n, \\ & \sum_{j} x_{ij} = 1, \ \forall i \in [k] \\ & x_{ij} \in \{0,1\}. \end{aligned}$$

[0077] The objective function $\sum_{i,j} S_{ij} x_{ij}$ effectively represents the average worst-case BER across all retained bits. To see that, consider that since the algorithm constrains on the total number of reliable bits $\sum_{i,j} \mathrm{HW}(C[j]) x_{ij}$, optimizing over the sum of BERs for reliable bits is the same as optimizing over the average BER. The constraint $\sum_j x_{ij} = 1$ implies that only one x_{ij} is assigned to 1, namely, each segment $\mathbf{M}[i]$ decodes to a unique codeword C_j.

[0078] A greedy heuristic can be applied to efficiently solve the proposed ILP problem via Lagrangian relaxation. The major challenge of the ILP formulation above lies in the constraint

$$\sum_{i,j} \mathrm{HW}(C[j]) x_{ij} \geq n,$$

which couples all decision variables x_{ij}'s. The standard technique in constrained optimization problems is to introduce Lagrangian regularizers to move complex constraints onto the objective function. After introducing a non-negative λ, the proposed ILP formation becomes

$$\begin{aligned} \min_{x_{ij}} \quad & \sum_{i,j} S_{ij} x_{ij} - \lambda \left(\sum_{i,j} \mathrm{HW}(C[j]) x_{ij} - n \right) \\ \text{s.t.} \quad & \sum_{j} x_{ij} = 1, \ \forall i \in [k] \\ & x_{ij} \in \{0,1\}. \end{aligned}$$

$L(\lambda)$ is denoted to be the optimal objective value with Lagrangian regularizer λ. By grouping terms with respect to x_{ij}'s, solving for $L(\lambda)$ can be decomposed into small sub-problems $L_i(\lambda)$'s only with decision variables $\{x_{i1}, x_{i2}, \ldots\}$ inside the i-th segment,

$$\begin{aligned} L_i(\lambda) = \min_{x_{ij}} \quad & \sum_{j} (S_{ij} - \lambda \, \mathrm{HW}(C[j])) x_{ij} \\ \text{s.t.} \quad & \sum_{j} x_{ij} = 1, \\ & x_{ij} \in \{0,1\}. \end{aligned}$$

[0079] Due to the binary constraints on x_{ij}, the i-th sub-problem $L_i(\lambda)$ identifies the index j with minimum $(S_{ij} - \lambda HW(C[j]))$:

$$x_{ij} = \begin{cases} 1 & j = \arg\min_k((S_{ik} - \lambda HW(C[k]))), \\ 0 & \text{otherwise.} \end{cases}$$

The optimal choice of λ can be found via efficient binary search in interval [0, 1]. Therefore, the greedy-based heuristic runs in near-linear time.

[0080] The approach discussed above leads to an optimal HDS reduction but requires a possibly expensive characterization effort in which the reliability information for each bit of every production PUF chip is extracted across all conditions.

[0081] The following is a discussion of a technique for an economically feasible process of bit-specific across-temperature BER characterization needed for HDS reduction and other fuzzy extractor optimization strategies, including lossy compression.

[0082] Figure 5 is a flowchart of a method 500 for bit-specific across-temperature BER characterization that enables HDS reduction and other fuzzy extractor optimizations in accordance with an embodiment of the present invention.

[0083] Referring to Figure 5, in conjunction with Figures 1-3, in step 501, a population-based analysis is performed to extract cell specific nominal one-probabilities and worst-case bit-error-rates at the technology development phase.

[0084] In step 502, statistics, such as the mean μ_ρ and standard deviation σ_ρ, of the worst-case bit-error-rates for cells under the same nominal one-probability ρ, are extracted at the technology development phase.

[0085] In step 503, only nominal one-probabilities for each cell are measured at the production phase.

[0086] In step 504, the extracted mean μ_p is used as input for a helper data size reduction method for cells with nominal p to select reliable bits at the production phase.

[0087] In step 505, the confidence level of the true effective BER (target BER) is computed at the production phase using only statistics extracted in the technology phase and nominal p's. The following discussion is based on the average of μ_p for selected reliable bits being computed

at the production phase but the present invention can utilize any other confidence level estimation tool. For example, the present invention may utilize $\bar{\mu}_p = \sum u_p/n$ for the selected set of reliable bits. Then an offset v is computed to satisfy $P(\bar{p}_w - \bar{\mu}_p > v) \leq \delta$ for a given confidence level δ via a stochastic concentration theory at the production phase. And then an error correction code with a corresponding target bit-error-rate is designed at the production phrase, where the target bit-error-rate is set for the error correction code as $p_t = \bar{\mu}_p + v$.

[0088] In step 506, the fuzzy extractor is optimized by identifying a subset of more reliable bits out of the population of PUF bits using the derived confidence level for the average across-temperature BER of the set of cells.

[0089] A more detailed discussion regarding method 500 is provided below.

[0090] Method 500 is a technique based on stochastic modeling of worst-case BERs to drive the lossy compression via measurements performed only under room temperature while allowing key reconstruction with overwhelmingly high probability. For every instance with obtained average BER $\bar{p}_w = \sum_{i=1}^{n} p_{wi}/n \leq p_t$, the reconstruction probability guarantee is met. Specifically, it is shown that for a practical number of cells involved, using the estimate of $\bar{p}_w$, this technique ensures that

$$\Pr(\bar{p}_w \leq p_t) \geq 1 - \delta,$$

in which δ << 1 is the fraction of PUF chips for which reliable reconstruction cannot be guaranteed. It is shown that δ can be set to a value that ensures almost-perfect reconstruction rate, for example, $\delta = 10^{-5}$.

[0091] This technique utilizes the correlation between maximum (worst-case) BERs with their nominal one-probabilities. Figure 6 is a graph depicting individual cell's maximum across-temperature BERs plotted against nominal-temperature one-probabilities in accordance with an embodiment of the present invention.

[0092] Such a technique includes performing a population-based analysis of SRAM cells at the technology development phase, to get for each cell the nominal one-probability p_i and worst-case p_{wi} with respect to enrollment under nominal temperature. For cells under each fixed nominal one-probability p, the average μ_p and standard deviation σ_p of worst-case p_w's are extracted. At the production phase, individual one-probabilities p_i's are measured under nominal temperature

for each chip. For cells with nominal p, we use μ_p to estimate p_w. Namely, $\{\mu_{p1}, \mu_{p2}, \ldots\}$ are sent into the HDS reduction strategies, including the lossy compression described above, instead of $\{p_{w1}, p_{w2}, \ldots\}$ to select SRAM bits as input to the fuzzy extractor. For the set of selected cells, μ_p is computed by $\bar{\mu}_p = \sum_{i=1}^{n} \mu_{pi}/n$. For given confidence level δ, an offset ν is computed to satisfy $P(\bar{p}_w - \bar{\mu}_p > \nu) \leq \delta$, via the Bennett's inequality in the stochastic concentration theory. Then the target BER for ECC of fuzzy extractors can be set as $p_t = \bar{\mu}_p + \nu$.

[0093] The offset ν can be obtained using stochastic concentration theory, and in one rendering of the present invention using the Bennett's inequality:

[0094] A computation based on the Bennett's inequality: Let $X_1, X_2, \ldots, X_n$ be independent random variables with zero mean, and $X_i \leq 1$ almost surely $\forall i \in [n]$. Let $\sigma^2 = \sum_{i=1}^{n} \mathrm{Var}(X_i)/n$. Then for any $t > 0$,

$$\Pr\left(\sum_{i=1}^{n} X_i > t\right) \leq \exp\left(-n\sigma^2 h\left(\frac{t}{n\sigma^2}\right)\right),$$

in which $h(u) = (1 + u)\log(1 + u) - u$ for $u > 0$.

[0095] $X_i = p_{wi} - \mu_{pi}$ denotes the deviation of p_{wi} from its predicted alternative μ_{pii}, and $\mathrm{Var}(X_i) = \sigma_{pi}^2$. The derivation $\bar{p}_w - \bar{\mu}_p$ is just $\sum_{i=1}^{n} X_i$. Take $t = \phi(n)\left(\sum_{i=1}^{n} \sigma_{pi}\right)$ and let the upper bound for all σ_p of selected SRAM cells to be σ,

$$\Pr(\bar{p}_w - \bar{\mu}_p > t) = \Pr\left(\sum_{i=1}^{n} X_i > \phi(n)\left(\sum_{i=1}^{n} \sigma_{pi}\right)\right)$$
$$\leq \exp\left(-n\sigma^2 h\left(\frac{\phi(n)}{\sigma}\right)\right).$$

Therefore, it is shown that with increase of n, $\bar{p}_w$ converges to $\bar{\mu}_p$ exponentially fast.

[0096] Second, for given n and δ, it is shown how to derive υ analytically and drive the flow iteratively by increasing n when the reliability guarantee is not met for current bit-selection. Under the proposed condition $\bar{\mu}_p + \nu \leq p_t$, the event $\bar{p}_w > p_t$ implies that $\bar{p}_w - \bar{\mu}_p > \nu$. Namely,

$$\Pr(\bar{p}_w > p_t) \leq \Pr(\bar{p}_w - \bar{\mu}_p > \nu).$$

[0097] In order to satisfy the constraint $\Pr(\bar{p}_w > p_t) < \delta$, it is sufficient to set $\upsilon = \phi(n)\sigma$ and get

$$Pr(\beta_w - \beta_b > w) \leq \exp(-n\sigma^2 h(\frac{\phi(n)}{\sigma})) \leq \delta$$

Optimal values of $\phi(n)$ and υ can be determined via the equation above.

[0098] As a result of the present invention, there is a dramatic reduction in the amount of helper data that needs to be stored in non-volatile memory and/or one-time-programmable memory, such as EPROM or e-Fuse. The cost of such memory is high in both silicon area (cost) and post-manufacture-time configuration. As a result of the present invention, memory consumption is reduced thereby improving the functionality or capability of a PUF system. That is, by reducing memory consumption, the efficiency of the PUF system is improved.

[0099] Furthermore, as a result of the present invention, the effective average BER that needs to be handled by error-correction coding within a fuzzy extractor is reduced. This allows a reduction of implementation cost of the fuzzy extractor.

[00100] Additionally, the present invention improves the prediction accuracy, i.e., the present invention reliability estimates the bit-error-rate of the physical unclonable function under environmental variations using high-dimensional stochastic modeling. The present invention is able to reliably estimate the worst-case error rate thereby allowing a significant cost (in terms of throughput, power, energy, silicon area, and price) reduction by enabling bit-selection based algorithms.

[00101] The following is a discussion of further applying the HDS reduction methods to strong PUFs.

[00102] Referring now to Figure 7, Figure 7 is a flowchart of a method 700 for helper data size reduction for strong PUFs in accordance with an embodiment of the present invention.

[00103] In step 701, pseudo random numbers are generated, for example, by using linear feedback shift registers. In one embodiment, a pre-defined sequence of m-bit binary strings is generated, where m corresponds to the number of challenge bits of the strong PUF. As a result, each state of the pseudo random generator corresponds to a unique challenge response pair for the strong PUF with its unique bit-error-rate.

[00104] In step 702, the generated pseudo random numbers are inputted to the strong PUF as challenges.

[00105] In step 703, the strong PUF outputs a sequence of responses to the given input challenges above that are stored in a one-dimensional indexed array. In one embodiment, each array element in the array corresponds to the response to a unique input challenge as the state of the pseudo random generator.

[00106] In step 704, the techniques of compression and economically-feasible confidence interval estimation are applied to form a most compact representation of the sufficiently reliable challenge response pairs of the strong PUF as entries of the abstract array.

[00107] In step 705, such a representation is stored as reduced helper data in memory (e.g., memory 104 of Figure 1) of a PUF system (e.g., PUF system 100 of Figure 1).

[00108] The descriptions of the various embodiments of the present invention have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. For example, many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described embodiments. The terminology used herein was chosen to best explain the principles of the embodiments, the practical application or technical improvement over technologies found in the marketplace, or to enable others of ordinary skill in the art to understand the embodiments disclosed herein.

CLAIMS:

1. A method for reducing the amount of helper data that needs to be stored, the method comprising:

determining individual cell bit-error-rates of a physical unclonable function;

formulating a lossy compression problem using said determined individual cell bit-error-rates of said physical unclonable function;

solving said formulated lossy compression problem;

storing a solution to said formulated lossy compression problem as a map representing reliable cells in a memory of a physical unclonable function system; and

constructing helper data to be utilized by a fuzzy extractor using said map representing reliable cells and error correction code helper data.

2. The method as recited in claim 1, wherein said lossy compression problem is an integer linear programming problem.

3. The method as recited in claim 2 further comprising:

generating a codebook using said determined individual cell bit-error-rates of said physical unclonable function;

formulating said lossy compression problem to seek an optimal mapping from memory segments into codewords in said generated codebook; and

using a Lagrangian relaxation method for solving said integer linear programming problem to reduce a number of bits of said helper data.

4. A computer program product for reducing the amount of helper data that needs to be stored, the computer program product comprising a computer readable storage medium having program code embodied therewith, the program code comprising the programming instructions for:

determining individual cell bit-error-rates of a physical unclonable function;

formulating a lossy compression problem using said determined individual cell bit-error-rates of said physical unclonable function;

solving said formulated lossy compression problem;

storing a solution to said formulated lossy compression problem as a map representing reliable cells in a memory of a physical unclonable function system; and

constructing helper data to be utilized by a fuzzy extractor using said map representing reliable cells and error correction code helper data.

5. The computer program product as recited in claim 4, wherein said lossy compression problem is an integer linear programming problem.

6. The computer program product as recited in claim 5, wherein the program code further comprises the programming instructions for:

generating a codebook using said determined individual cell bit-error-rates of said physical unclonable function;

formulating said lossy compression problem to seek an optimal mapping from memory segments into codewords in said generated codebook; and

using a Lagrangian relaxation method for solving said integer linear programming problem to reduce a number of bits of said helper data.

7. A system, comprising:

a memory unit for storing a computer program for reducing the amount of helper data that needs to be stored; and

a processor coupled to the memory unit, wherein the processor is configured to execute the program instructions of the computer program comprising:

determining individual cell bit-error-rates of a physical unclonable function;

formulating a lossy compression problem using said determined individual cell bit-error-rates of said physical unclonable function;

solving said formulated lossy compression problem;

storing a solution to said formulated lossy compression problem as a map representing reliable cells in a memory of a physical unclonable function system; and

constructing helper data to be utilized by a fuzzy extractor using said map representing reliable cells and error correction code helper data.

8. The system as recited in claim 7, wherein said lossy compression problem is an integer linear programming problem.

9. The system as recited in claim 8, wherein the program instructions of the computer program further comprise:

generating a codebook using said determined individual cell bit-error-rates of said physical unclonable function;

formulating said lossy compression problem to seek an optimal mapping from memory segments into codewords in said generated codebook; and

using a Lagrangian relaxation method for solving said integer linear programming problem to reduce a number of bits of said helper data.

10. A method for reducing the amount of helper data that needs to be stored, the method comprising:

extracting distribution of cells' across-temperature bit-error-rates using a population-based analysis at a technology development phase;

measuring only nominal one-probabilities for each cell at a production phase;

using said population-based analysis of said cells' across-temperature bit-error-rates for said measured nominal one-probabilities for each cell to derive a confidence level for an average across-temperature bit-error-rate of a set of cells; and

optimizing a fuzzy extractor by identifying a subset of more reliable bits out of a population of physical unclonable function bits using said derived confidence level for said average across-temperature bit-error-rate of said set of cells.

11. The method as recited in claim 10, wherein said confidence level is derived by solving an inequality based on stochasitic concentration theory.

12. The method as recited in claim 11, wherein said stochastic concentration theory comprises Bennett's inequality.

13. A computer program product for reducing the amount of helper data that needs to be stored, the computer program product comprising a computer readable storage medium having program code embodied therewith, the program code comprising the programming instructions for:

extracting distribution of cells' across-temperature bit-error-rates using a population-based analysis at a technology development phase;

measuring only nominal one-probabilities for each cell at a production phase;

using said population-based analysis of said cells' across-temperature bit-error-rates for said measured nominal one-probabilities for each cell to derive a confidence level for an average across-temperature bit-error-rate of a set of cells; and

optimizing a fuzzy extractor by identifying a subset of more reliable bits out of a population of physical unclonable function bits using said derived confidence level for said average across-temperature bit-error-rate of said set of cells.

14. The computer program product as recited in claim 13, wherein said confidence level is derived by solving an inequality based on stochasitic concentration theory.

15. The computer program product as recited in claim 14, wherein said stochastic concentration theory comprises Bennett's inequality.

16. A system, comprising:

a memory unit for storing a computer program for reducing the amount of helper data that needs to be stored; and

a processor coupled to the memory unit, wherein the processor is configured to execute the program instructions of the computer program comprising:

extracting distribution of cells' across-temperature bit-error-rates using a population-based analysis at a technology development phase;

measuring only nominal one-probabilities for each cell at a production phase;

using said population-based analysis of said cells' across-temperature bit-error-rates for said measured nominal one-probabilities for each cell to derive a confidence level for an average across-temperature bit-error-rate of a set of cells; and

optimizing a fuzzy extractor by identifying a subset of more reliable bits out of a population of physical unclonable function bits using said derived confidence level for said average across-temperature bit-error-rate of said set of cells.

17. The system as recited in claim 16, wherein said confidence level is derived by solving an inequality based on stochasitic concentration theory.

18. The system as recited in claim 17, wherein said stochastic concentration theory comprises Bennett's inequality.

19. A method for helper data size reduction for strong physical unclonable functions, the method comprising:

generating pseudo random numbers;

inputting said generated pseudo random numbers to a strong physical unclonable function which outputs a set of responses to said inputted pseudo random numbers as input challenges that are stored in a one-dimensional indexed array;

applying compression and confidence interval estimation techniques to form a compact representation of challenge response pairs of said strong physical unclonable function as entries of said array; and

storing said representation as reduced helper data in a memory of a physical unclonable function system.

20. The method as recited in claim 19, wherein said pseudo random numbers are generated by a pseudo random generator as a pre-defined sequence of m-bit binary strings, where m corresponds to a number of challenge bits of said strong physical unclonable function.

21. The method as recited in claim 20, wherein each state of said pseudo random generator corresponds to a unique challenge response pair for said strong physical unclonable function with its unique bit-error-rate.

22. The method as recited in claim 20, wherein each element in said array corresponds to a response to a unique state of said pseudo random generator.

23. A computer program product for helper data size reduction for strong physical unclonable functions, the computer program product comprising a computer readable storage medium having program code embodied therewith, the program code comprising the programming instructions for:

generating pseudo random numbers;

inputting said generated pseudo random numbers to a strong physical unclonable function which outputs a set of responses to said inputted pseudo random numbers as input challenges that are stored in a one-dimensional indexed array;

applying compression and confidence interval estimation techniques to form a compact representation of challenge response pairs of said strong physical unclonable function as entries of said array; and

storing said representation as reduced helper data in a memory of a physical unclonable function system.

24. The computer program product as recited in claim 23, wherein said pseudo random numbers are generated by a pseudo random generator as a pre-defined sequence of m-bit binary strings, where m corresponds to a number of challenge bits of said strong physical unclonable function.

25. The computer program product as recited in claim 24, wherein each state of said pseudo random generator corresponds to a unique challenge response pair for said strong physical unclonable function with its unique bit-error-rate.

26. The computer program product as recited in claim 24, wherein each element in said array corresponds to a response to a unique state of said pseudo random generator.

27. A system, comprising:

a memory unit for storing a computer program for helper data size reduction for strong physical unclonable functions; and

a processor coupled to the memory unit, wherein the processor is configured to execute the program instructions of the computer program comprising:

generating pseudo random numbers;

inputting said generated pseudo random numbers to a strong physical unclonable function which outputs a set of responses to said inputted pseudo random numbers as input challenges that are stored in a one-dimensional indexed array;

applying compression and confidence interval estimation techniques to form a compact representation of challenge response pairs of said strong physical unclonable function as entries of said array; and

storing said representation as reduced helper data in a memory of a physical unclonable function system.

28. The system as recited in claim 27, wherein said pseudo random numbers are generated by a pseudo random generator as a pre-defined sequence of m-bit binary strings, where m corresponds to a number of challenge bits of said strong physical unclonable function.

29. The system as recited in claim 28, wherein each state of said pseudo random generator corresponds to a unique challenge response pair for said strong physical unclonable function with its unique bit-error-rate.

30. The system as recited in claim 28, wherein each element in said array corresponds to a response to a unique state of said pseudo random generator.

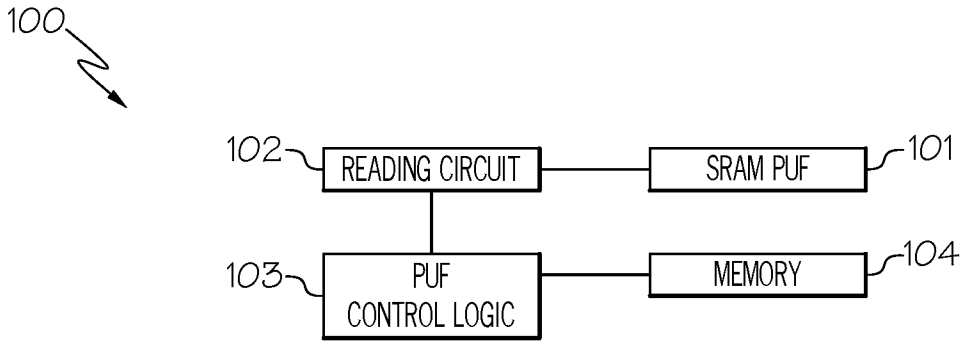

100
102
READING CIRCUIT
SRAM PUF
101
103
PUF
CONTROL LOGIC
MEMORY
104

FIG. 1

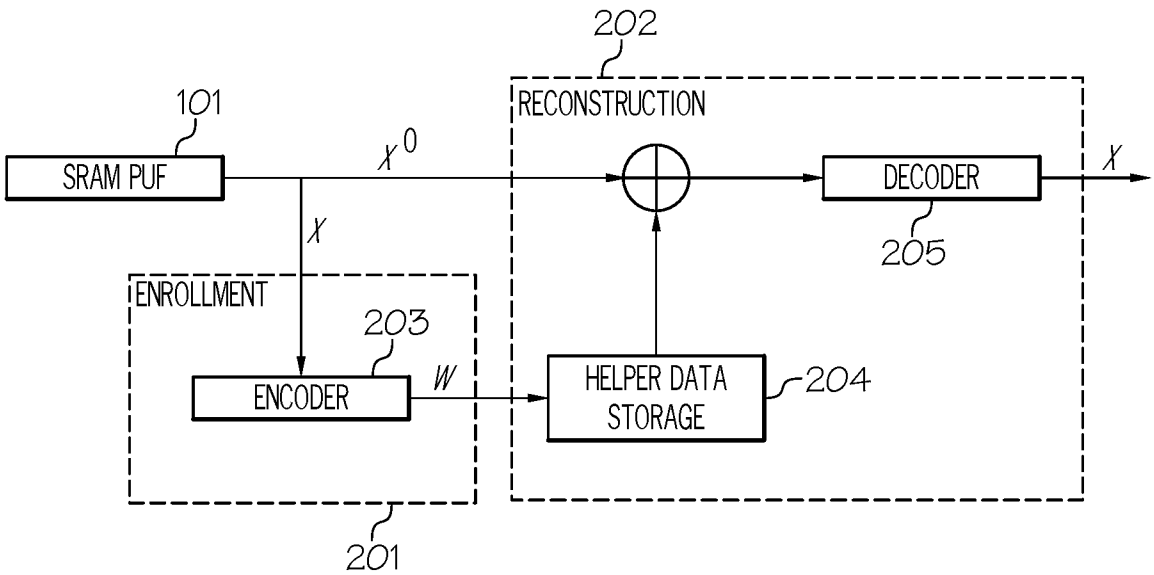

202
RECONSTRUCTION
101
SRAM PUF
X^0
X
DECODER
205
ENROLLMENT
203
ENCODER
W
HELPER DATA STORAGE
204
201

FIG. 2

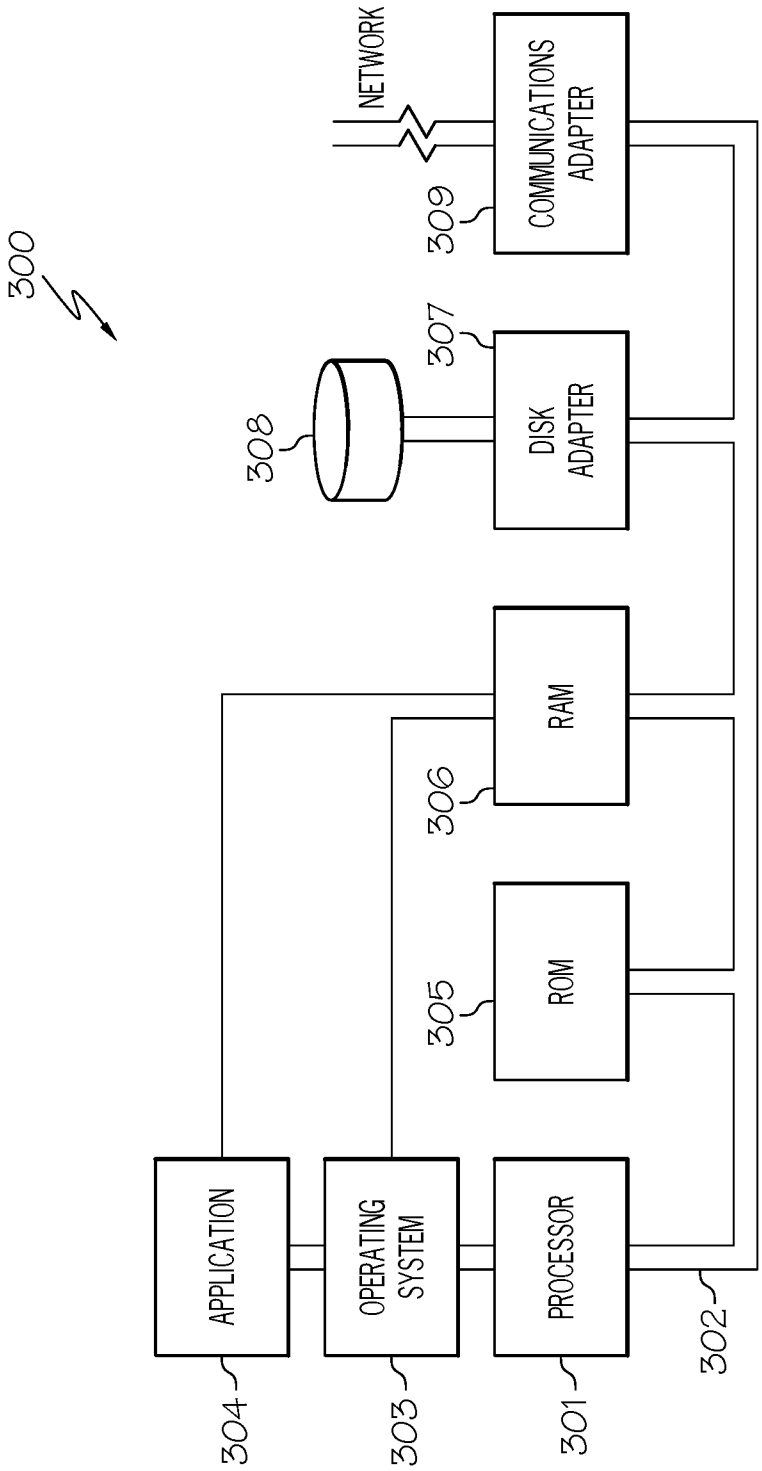

300
NETWORK
COMMUNICATIONS ADAPTER
309
DISK ADAPTER
307
308
RAM
306
ROM
305
APPLICATION
OPERATING SYSTEM
PROCESSOR
304
303
301
302

FIG. 3

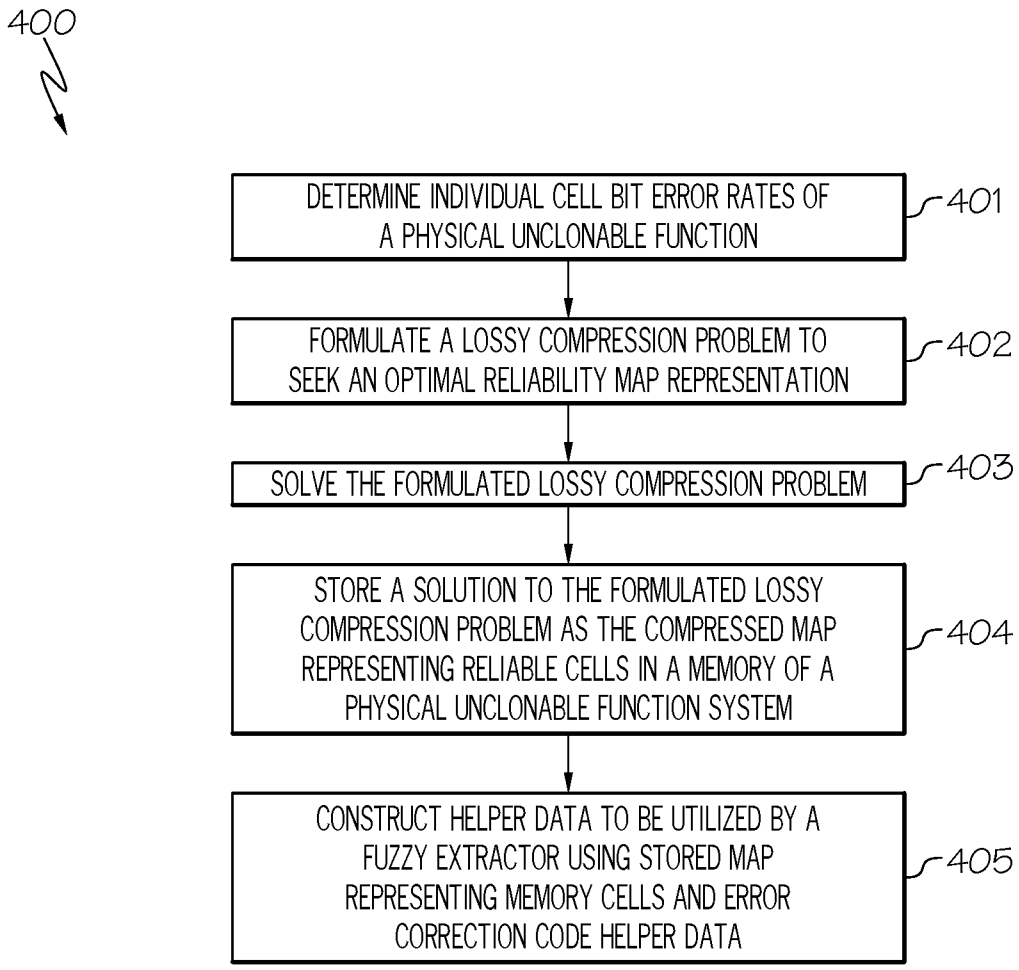

400
DETERMINE INDIVIDUAL CELL BIT ERROR RATES OF A PHYSICAL UNCLONABLE FUNCTION
401
FORMULATE A LOSSY COMPRESSION PROBLEM TO SEEK AN OPTIMAL RELIABILITY MAP REPRESENTATION
402
SOLVE THE FORMULATED LOSSY COMPRESSION PROBLEM
403
STORE A SOLUTION TO THE FORMULATED LOSSY COMPRESSION PROBLEM AS THE COMPRESSED MAP REPRESENTING RELIABLE CELLS IN A MEMORY OF A PHYSICAL UNCLONABLE FUNCTION SYSTEM
404
CONSTRUCT HELPER DATA TO BE UTILIZED BY A FUZZY EXTRACTOR USING STORED MAP REPRESENTING MEMORY CELLS AND ERROR CORRECTION CODE HELPER DATA
405

FIG. 4

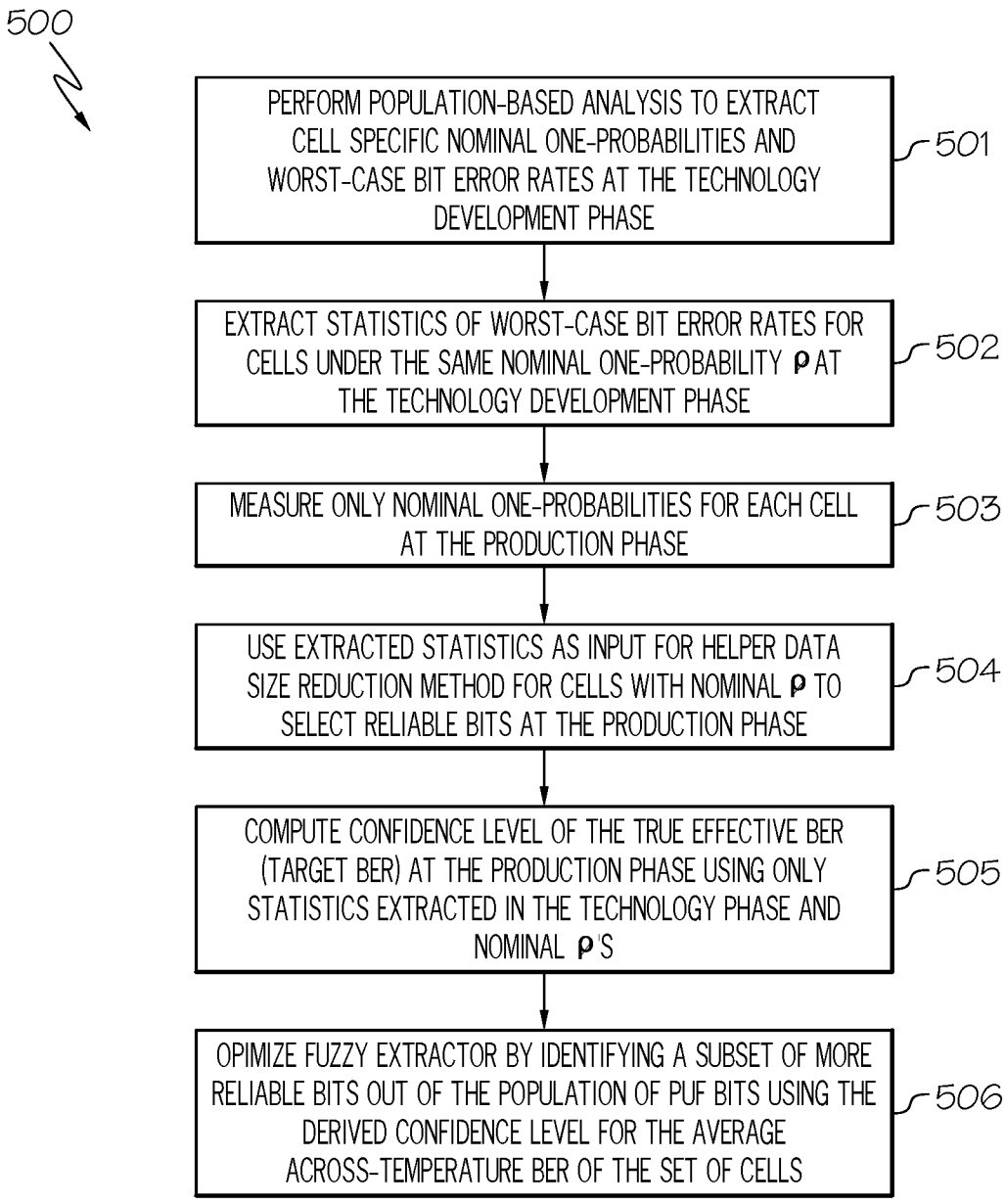

500
PERFORM POPULATION-BASED ANALYSIS TO EXTRACT CELL SPECIFIC NOMINAL ONE-PROBABILITIES AND WORST-CASE BIT ERROR RATES AT THE TECHNOLOGY DEVELOPMENT PHASE
501
EXTRACT STATISTICS OF WORST-CASE BIT ERROR RATES FOR CELLS UNDER THE SAME NOMINAL ONE-PROBABILITY ρ AT THE TECHNOLOGY DEVELOPMENT PHASE
502
MEASURE ONLY NOMINAL ONE-PROBABILITIES FOR EACH CELL AT THE PRODUCTION PHASE
503
USE EXTRACTED STATISTICS AS INPUT FOR HELPER DATA SIZE REDUCTION METHOD FOR CELLS WITH NOMINAL ρ TO SELECT RELIABLE BITS AT THE PRODUCTION PHASE
504
COMPUTE CONFIDENCE LEVEL OF THE TRUE EFFECTIVE BER (TARGET BER) AT THE PRODUCTION PHASE USING ONLY STATISTICS EXTRACTED IN THE TECHNOLOGY PHASE AND NOMINAL ρ'S
505
OPIMIZE FUZZY EXTRACTOR BY IDENTIFYING A SUBSET OF MORE RELIABLE BITS OUT OF THE POPULATION OF PUF BITS USING THE DERIVED CONFIDENCE LEVEL FOR THE AVERAGE ACROSS-TEMPERATURE BER OF THE SET OF CELLS
506

FIG. 5

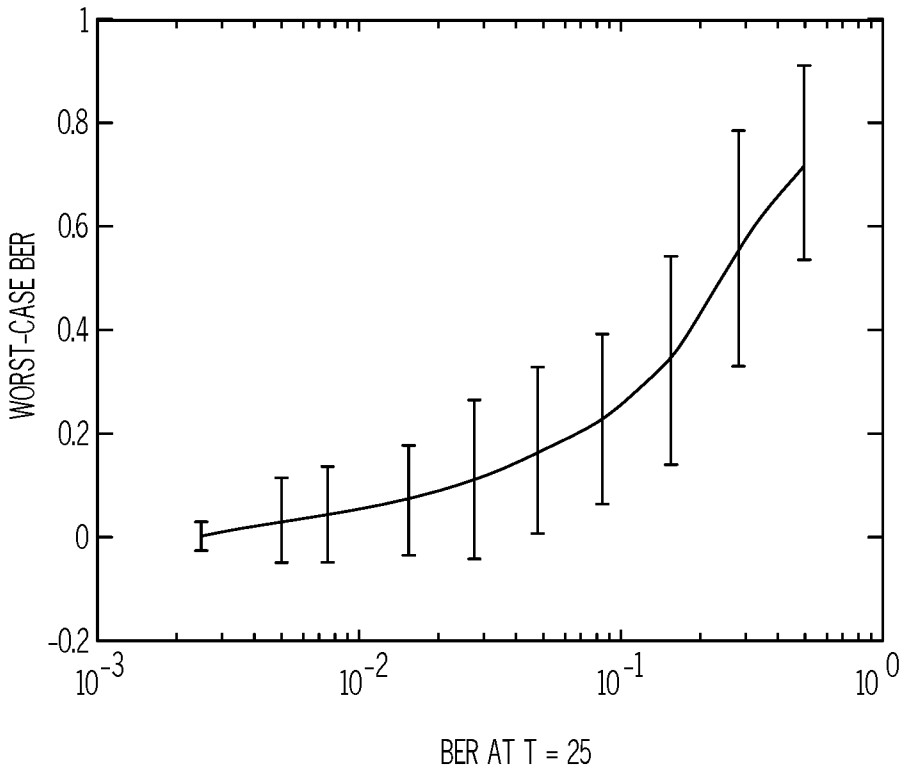


FIG. 6

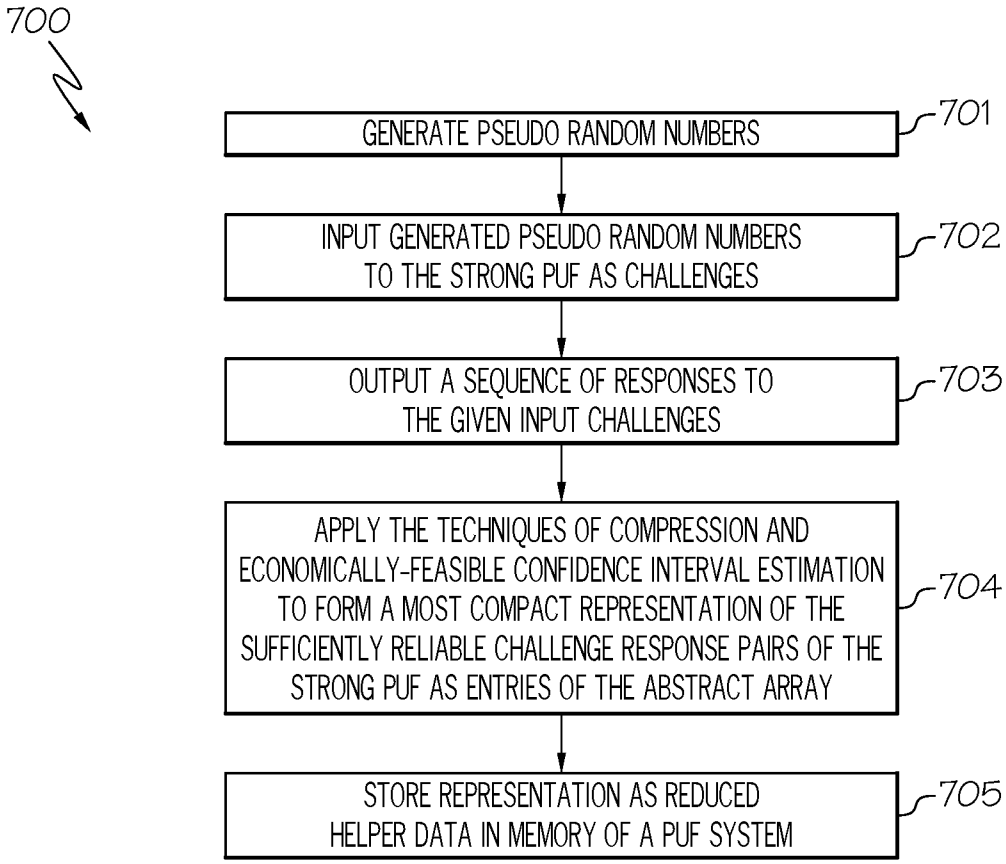

700
GENERATE PSEUDO RANDOM NUMBERS
701
INPUT GENERATED PSEUDO RANDOM NUMBERS TO THE STRONG PUF AS CHALLENGES
702
OUTPUT A SEQUENCE OF RESPONSES TO THE GIVEN INPUT CHALLENGES
703
APPLY THE TECHNIQUES OF COMPRESSION AND ECONOMICALLY-FEASIBLE CONFIDENCE INTERVAL ESTIMATION TO FORM A MOST COMPACT REPRESENTATION OF THE SUFFICIENTLY RELIABLE CHALLENGE RESPONSE PAIRS OF THE STRONG PUF AS ENTRIES OF THE ABSTRACT ARRAY
704
STORE REPRESENTATION AS REDUCED HELPER DATA IN MEMORY OF A PUF SYSTEM
705

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 18/24952

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H03M 13/00 (2018.01)
CPC - H04L 1/0042, H03M 13/03, H04L 9/3278, H04L 2209/34

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
See Search History Document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
See Search History Document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History Document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 2,773,061 B1 (Fraunhofer Ges Zur Forderung Der Angewandten Forschung E V) 03 September 2014 (03.09.2014) entire document (especially pg. 3, para [0001]; pg. 7, para [0030]; pg. 10, para [0046]; pg. 13, para [0069] - [0070]; pg. 13, para [0072], pg. 16, para [0098] -[0099], pg. 17, para [0101] ; pg. 17,para [0106]);	1-9
Y	Hiller, Matthias. Key derivation with physical unclonable functions. [online] published 2016. [retrieved on 17 July 2018 (17.07.2018)] Retrieved from the Internet <URL:https://mediatum.ub.tum.de/doc/1311665/file.pdf> entire document (especially pg. 38 to pg. 39; pg. 45; pg. 58 to pg. 60; pg. 69; pg. 66 to pg. 67; pg. 76 to pg. 77 pg. 115 to pg. 117)	1-9
Y	Salamatian, et al. "Maximum Entropy Functions: Approximate Gacs-Korner for Distributed Compression." [online] published April 13, 2016. [retrieved on 17 July 2018 (17.07.2018)] Retrieved from the Internet<URL:https://arxiv.org/pdf/1604.03877.pdf> (pg. 5, col. 1).	3, 6, 9
A	US 2016/0182045 A1 (Carnegie Mellon University) 23 June 2016 (23.06.2016) entire document	1-9

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 July 2018 (17.07.2018)	31 JUL 2018
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 18/24952

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

-see extra shet-

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-9

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 18/24952

Continuation of Box III: Lack of Unity

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I: Claims 1-9 are drawn to storing a solution of a formulated lossy compression problem using a determined individual cell bit-error-rates of the physical unclonable function in order to construct help data that is used by a fuzzy extractor.

Group II: Claims 10-18 are drawn to reducing the amount of stored helper data; deriving a confidence level by measuring only nominal one-probabilities for each extracted cell across-temperature bit-error-rates at a production phase; and optimizing a fuzzy extractor identifying a subset of more reliable bits.

Group III: Claims 19-30 are drawn to inputting the generated pseudo random numbers into a strong physical unclonable function; storing the output in a one-dimensional indexed array and forming compact representation of challenge response pairs by applying compression and confidence interval estimation techniques, which is stored in the array and storing the representation as reduced helper data.

The inventions listed as Groups I through III do not relate to a single general inventive concept under PCT Rule 13.1 because under PCT Rule 13.2 they lack the same or corresponding technical features for the following reasons:

Special Technical Features:
The special technical feature of Group I is storing a solution of a formulated lossy compression problem using a determined individual cell 8 bit-error-rates of the physical unclonable function in order to construct help data that is used by a fuzzy extractor , not present in any other group.

The special technical feature of Group II is reducing the amount of stored helper data; deriving a confidence level by measuring only nominal one-probabilities for each extracted cell across-temperature bit-error-rates at a production phase; and optimizing a fuzzy extractor identifying a subset of more reliable bits, not present in any other group.

The special technical feature of Group III is inputting the generated pseudo random numbers into a strong physical unclonable function; storing the output in a one-dimensional indexed array and forming compact representation of challenge response pairs by applying compression and confidence interval estimation techniques, which is stored in the array and storing the representation as reduced helper data, not present in any other group.

Common Technical Features:

-Groups I through III share the technical feature of a system/method/computer program product, comprising: a memory unit for storing a computer program for helper data size reduction for strong physical unclonable functions; and a processor coupled to the memory unit, wherein the processor is configured to execute the program instructions of the computer program comprising: cell bit-error-rates of a physical unclonable function. However, this shared technical features does not represent a contribution over

EP 2,773,061 B1 (Fraunhofer Ges Zur Forderung Der Angewandten Forschung E V) (hereinafter Fraunhofer) 03 September 2014 (03.09.2014).

Fraunhofer teaches a system/method/computer program product (pg. 3, para [0001]; pg. 10, para [0046]; pg. 17, para [0101]), comprising: a memory unit for storing a computer program for helper data size reduction for strong physical unclonable functions (e.g. Storing the relative distance between the used PUF responses may reduce the size of the helper data significantly, compared to storing t; he absolute position, pg. 16, para [0098]-[0099]; pg. 17, para [0110]); and a processor coupled to the memory unit, wherein the processor is configured to execute the program instructions of the computer program (e.g. computer readable medium and so executed by a computer or processor, pg. 17, para [0110]) comprising:
cell bit-error-rates of a physical unclonable function (e.g. the number of response values (PUF Outputs) per key bit of the secret information and bounded or simulated bit error probabilities for several fuzzy extractors, pg. 16, para [0096]).

-Groups I and II share the technical feature of fuzzy extractor; and reliable bits/cells. However, this shared technical features does not represent a contribution over Fraunhofer.

Fraunhofer teaches fuzzy extractor (e,g. simulated bit error probabilities for several fuzzy extractors, i.e. for several methods for deriving secret information from response values. Previous approaches are visualized by unconnected points and the values interconnected by bold lines show the result of the previously described our new DSC fuzzy extractor, pg. 16, para [0096]; pg. 14, para [0079]); and reliable bits/cells (e.g. the reliability of the PUF Outputs within each block is subject to the process variation. Some DSC embodiments follow a different approach by defining a reliability or another predetermined criterion and adapting the block size for every code sequence bit to the stochastic process. One goal of DSC is to reduce the statistical variation in the reliability of the PUF Outputs that are used for key reproduction, pg. 7, para [0030]; pg. 12, para [0069]-[0070]).

-Continuation in next extra sheet-

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 18/24952

-Continuation in preceding extra sheet-

-Groups I and III share the technical feature of compression. However, this shared technical features does not represent a contribution over

Fraunhofer in view of US 2016/0182045 A1 (Carnegie Mellon University) (hereinafter Carnegie) 23 June 2016 (23.06.2016)

Fraunhofer fails to teach compression.
However, Carnegie, in an analogous art, teaches compression (e.g.stressing can increase a probability of the PUF circuit for resolving to a certain output value over a plurality of operating conditions (e.g., different temperature, atmospheric pressure, moisture, physical strain and/or compression conditions), para [0040]). It would have been obvious to one of ordinary skill in the art to have modified the system of Fraunhofer by including cell bit-error-rates of a physical unclonable function as taught by Carnegie because the modification would increase a probability of the PUF circuit for resolving to a certain output value over a plurality of operating conditions (Carnegie , para [0040]).

Thus, unity of invention is lacking under PCT Rule 13.1 because Groups I-III do not share a same or corresponding special technical feature that would provide a unifying contribution over the prior art. None of these special technical features are common to the other groups.