DESIGN OF PUFS FROM SENSORS AND THEIR CALIBRATION

FIELD OF THE INVENTION

[0001] The present invention generally relates to cybersecurity and more specifically to creating and authenticating physically unclonable functions (PUFs) which may be a calibrated sensor or a pair of sensors.

SUMMARY OF THE INVENTION

[0002] Sensors convert physical and/or chemical signals into electric signals driving microelectronic systems. In order to generate electric signals that accurately represent the physical or chemical signals, calibration techniques have to compensate for the natural variations which are created during the manufacturing of the sensors. In this disclosure several methods are used to exploit the natural physical variations of sensors, to generate cryptographic physically unclonable functions (PUF) that are aimed at strengthening the cybersecurity of microelectronic systems.

[0003] The first architecture disclosed herein is based on the extraction of a stream of bits from the calibration table of each sensor to generate reference patterns, called PUF challenges, which can be stored in secure servers. The authentication of the sensor is positive when the data streams that are generated on demand, called PUF responses, match the challenges. To prevent a malicious party from generating responses, instructions can be added as part of the PUF challenges to define which parts of the calibration tables are to be used for response generation, and what additional responses can be generated by the embedded RAMs.

[0004] The second authentication architecture that is disclosed is based on differential sensors, one of them having the calibration module disconnected. The response to a physical or chemical signal from such a sensor can then be used to authenticate a specific pair of sensors.

[0005] The above features and advantages of the present invention will be better understood from the following detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1 is a block diagram of a sensor system.

[0007] FIG. 2 is a block diagram of a calibration of a sensor system.

[0008] FIG. 3 is a block diagram of a prior art> sensor PUF system.

[0009] FIG. 4 is an illustration of a set of calibration tables.

[0010] FIG. 5 is a PUF generator based on calibration tables.

[0011] FIG. 6 illustrates a method of hiding the location of the PUF generation within a calibration table.

[0012] FIG. 7 illustrates a PUF generation with calibration table & SRAM.

[0013] FIG. 8 illustrates a PUF generation: example of challenge-response-pair matching.

[0014] FIG. 9 illustrates a differential PUF generator.

[0015] FIG. 10 illustrates differential PUF generator-signal processing.

DETAILED DESCRIPTION

[0016] The present inventions will now be discussed in detail with regard to the attached drawing figures that were briefly described above. In the following description, numerous specific details are set forth illustrating the Applicant’s best mode for practicing the invention and enabling one of ordinary skill in the art to make and use the invention. It will be obvious, however, to one skilled in the art that the present invention may be practiced without many of these specific details.

In other instances, well-known machines, structures, and method steps have not been described in particular detail in order to avoid unnecessarily obscuring the present invention. Unless otherwise indicated, like parts and method steps are referred to with like reference numerals.

[0017] ***Calibration of sensor devices.*** Sensor devices are increasingly integrated into electronic systems such as mobile devices, Internet of things (IoT), cyber physical systems (CPS), smart grid, medical devices, and safety components. The range of physical and chemical parameters that are converted into usable electronic signals is extremely pervasive, and includes acceleration, rotation, deviation to the magnetic north, electronic currents, motion, image, chemical and biochemical elements, blood composition, heart beat rate, temperature, pressure, mechanical stress, humidity, and many others. In Fig. 1, a block diagram of a sensor system is presented.

[0018] The sensing element transforms the physical signal into an analog electrical signal that is converted to a digital signal with an analog to digital conversion circuit. The digital processor should communicate to the external system an accurate representation of the physical signal. As shown in Fig. 2, sensor systems need to be calibrated with known physical signals producing known electrical signals. This includes a reset position, i.e. obtaining a zero as an output signal when no physical parameter is sensed, to correct deviations for accurate reading, and enhance the linearity of the electric signal. Others corrections that are often part of the calibration process can include adjusting temperature coefficients, biasing conditions, and cancelling background noise. A calibration table stored in a non-volatile memory may contain the information needed to produce quality signals out of each sensor.

[0019] ***Protection of sensor systems from cyber-attacks***. Very often sensor based systems that are connected to the web are vulnerable to cyber-attacks which could trigger life threatening conditions. Physically unclonable functions (PUF) can offer effective solutions to protect electronic systems from cyber-attacks. *InvenSense* and *Intrinsic-ID* announced in November 2015 a new secure architecture, “*TrustedSensors*” which is based on physically unclonable functions (PUF) generated by the static random access memories (SRAM) that are embedded in the sensor system. These PUFs act as digital finger prints leveraging the natural manufacturing variations that make every cell of an SRAM slightly different from each other’s. This allows cryptographic methods implemented on the network to enhance the trustworthiness of the authentication of the sensor system, and may thereby prevent cyber-attacks.

[0020] ***SRAM based Physically Unclonable Functions*** have been successfully implemented to strengthen the level of security of the authentication of electronic systems because SRAM memories are present in many electronic systems. The underlying mechanism of PUF is the creation of a large number of Challenge (i.e. Input) Response (i.e. output) Pairs (called CRPs) which are unique to each device. Once deployed during the authentication cycles, the PUFs are queried with challenges. The authentication is granted when the rate of matching responses is statistically high enough. Each SRAM cell is a flip flop that has in theory, an equal opportunity to be a zero or a one when powered up, however due to small asymmetries created during manufacturing, one side is usually preferred. An array of SRAM cells will then have a preferred response when powered which is exploited to generate PUF challenge-response pairs. SRAM based PUFs due to their popularity also attract crypto-analysts who have developed methods to break them and extract the responses. As a result, it has to be expected that in the future these SRAM PUFs might become increasingly weaker as cyber-protection.

[0021] Some sensor systems are based on open loop architectures such as the one shown in Fig. 3. The authentication is based on providing a known physical or chemical signal, and to compare the output signal, i.e. the response, with a reference, i.e. the challenge. The cryptographic protocol is based on the initial storage of the challenge in the secure terminal, to then compare it to the response produced during authentication. If the hamming distance between challenge and response (also referred as the CRP error rate) is low, the authentication is positive.

Each sensor is physically different from other sensors, so the authentications have a large probability to be negative unless the challenges and the responses are generated by the same sensor.

[0022] Variations due to aging, temperature, unstable physical or chemical signals, and/or noise weaken such architecture. The novel methods disclosed in this document have the objective to reduce the effect of these variations and enhance security.

[0023] Use of calibration tables to generate PUFs

[0024] The first novel method disclosed in this document is based on exploiting the calibration tables of a set of sensors that vary sensor to sensor due to natural excursions created during manufacturing. As shown in Fig. 4 each of the n different sensors have their own calibration table. There is no guarantee that two distinct sensors have distinct calibration tables, however the natural randomness makes these calibration tables unpredictable from each other’s tables, and good candidates for PUF challenges and responses generation.

[0025] Cryptographic protocols based on calibration tables

[0026] Fig. 5 shows the overall cryptographic protocol between a secure terminal and the sensor system. The calibration table that is stored in a non-volatile memory contains a stream of binary bits which is used to convert the signal produced by the sensing element, into a calibrated signal. Typically the lengths of the streams of binary bits vary from 8 bits to 256 bits depending on the complexity of the sensing element. The novel PUF challenges and responses are generated from the streams of binary bits stored in the calibration tables. To set up the initial cryptographic protocol, the reference data streams, the challenges, are transferred to the secure server. To authenticate the sensor system, the PUF generator reads again the calibration table to extract PUF responses which are then compared to the challenges. The method described here is working in a way similar to the way SRAM PUFs work, i.e., the randomness is coming from the calibration tables, rather than from the SRAMs after powering the system. The communication between the sensor system and the secure terminal has to be encrypted to prevent exposure to third parties.

[0027] Strengthening security

[0028] The level of exposure to third party attempts to extract PUF responses from the calibration table could be much lower than the SRAM based PUF if the non-volatile memory (NVM) storing the calibration table is dense and low power. This would be the case if the NVM is a resistive RAM, or ferroelectric RAM. The cell sizes of such NVMs are typically an order of magnitude smaller than SRAM cells, and much more difficult to observe. To further lower the exposure, two methods are described, i) hiding the PUF responses within the calibration table, and ii) multi-PUF architectures.

[0029] ***Hiding the PUF responses***. As exemplified in Fig. 6 the data stream stored as part of the calibration table can be re-ordered and selectively extracted to generate PUF responses. The instructions on how to reorder and extract the PUF can be part of the challenges. This increases the level of security in case a hacker finds a way through side channel attacks to read the calibration table. With lack of instructions, the hacker faces the difficulty of finding out where to read the responses within the calibration tables, which becomes difficult when the size of the NVMs storing the calibration table is large enough.

[0030] ***Multi-PUF architecture.*** Most sensor systems are designed with both NVM that store calibration tables and SRAM cache memories. As described in Fig. 7 it is then possible to have access to multi-PUF generation systems, the one described above using calibration tables together with the SRAM based PUFs. The expected result is to increase entropy, or the number of possible combinations, and thereby further increase the difficulty for a third party to extract the response from the system.

[0031] There are many possible embodiments of this disclosure to strengthen the level of security of a sensor system and hide the PUF responses from a hacker. In Fig. 8 the cryptographic protocol described is based on challenges which are data streams of binary bits with three sections: 1) the first section contain the digital instructions on what addresses the calibration table and the SRAM are to use to generate the responses (the digital instructions can also contain general information on how to generate the responses); 2) the second section contains the reference patterns, i.e. the challenges, that were generated out of the calibration table and 3) the third section contains the challenges generated out of the SRAM. The authentication is positive when the challenge-response-pairs (CRP) match. The use of the SRAM based PUF to strengthen the level of security, is given only as an example as other PUFs can be generated from sensor systems such as PUF generated from sensor PUFs, ring oscillators, gate delays, or NVMs. It also has to be noted that the three sections of the challenges described in Fig. 8, do not have to be nicely ordered in a serial way. For example the data stream can be mixed with random numbers and then decrypted for response generation.

[0032] **PUFs exploiting differential sensors**

[0033] The methods described in this section exploit the random physical properties of a pair of sensors. Electrical signals responding to physical or chemical signals are expected to differ sensor to sensor, while the purpose of calibration is to make all sensors look identical and accurate.

[0034] **Description of close loop sensor PUFs**

[0035] The closed loop method described in Fig. 9 is based on differential measurements. In this architecture two different sensors are integrated in the same system. One sensor is fully calibrated and produces electrical signals which accurately represent the physical or chemical signal that is activating the sensor.

[0036] The second sensor, also called the PUF sensor, is raw without calibration. The hamming distance between the first calibrated sensor and the second non-calibrated sensor (the PUF sensor) measures the excursion of the second sensor from the expected calibrated output. This hamming distance can be used as a PUF challenge-response-pair generator.

[0037] Let us define this system using a stream of binary bits. If the stream resulting from the calibrated sensor is B as the base:

[0038] $B = \{b_1, b_2, \ldots, b_i, \ldots, b_n\}$

[0039] If the stream resulting from the un-calibrated sensor is I like input:

[0040] $I = \{i_1, i_2, \ldots, i_i, \ldots i_n\}$

[0041] The response is given by:

[0042] $R = B \oplus I = \{r_1, r_2, \ldots, r_i, \ldots r_n\}$

[0043] With $\oplus$ been the logical exclusive OR (XOR) function and for $i \in \{1$ to $n\}$:

[0044] $r_i = b_i \oplus i_i$

[0045] The response R may then be compared with the challenge C stored in the secure terminal. C is generated during the initial set up in the same way R is generated during each authentication process. The authentication is positive when the response R and the challenge C match. The match is positive when the hamming distance between R and C is small. The hamming distance, or CRP errors, is the number of bits at “1” present in the resulting stream $R \oplus C$.

[0046] In addition, cryptographic techniques which hide the responses from potential hackers could be very important. One of these cryptographic methods is to use a hash function with random numbers to transmit the encrypted responses.

[0047] Modes of operation and examples.

[0048] ***Linear operations***. Assuming that both sensors in a closed loop architecture can operate within their linear region, the hamming distance between them stays constant when the physical or chemical signals are drifting. The two sensors are producing drifting electrical signals, however the distance between then stay constant. So, unlike open loop sensors, differential sensors can operate without known physical or chemical signals. This can enlarge the field of use of the novel method. The following examples are presented to better explain closed loop methods in the linear region of operation.

[0049] ***Example #1: securing the smart grid***. Uncalibrated current sensors (magnetometers) paired with calibrated sensors can be installed at every node of a grid. The hamming distance between the two output signals responding to a reference current Iref are the challenges and may be stored in the secure server managing the network. To authenticate a particular node, the reference current Iref is sent again to the node and the response to the current sensors is analyzed for CRP matching. This method can authenticate each sensor and conversely can be used at the node level to authenticate the network; in this last case the authentication is done by a secure processor that is part of the node.

[0050] ***Example #2: user authentication***. Each user is given a token that includes a pair of 3D magnetic sensors, and a small wireless communication apparatus. For authentication the user may place the token on a transmitter of a magnetic field of known amplitude that is located at the point of entry of a secure facility. The sensor placed in the token will read the magnetic field and transmit back the response to the transmitter for the CRP analysis which is done by the server of the secure facility. The identification of the user is preferably done with a different method that is synergistic with this authentication.

[0051] ***Example #3: authentication of smart phones***. Commercial smart phones incorporate multiple sensors such as accelerometers, gyroscopes, and magnetometers. The insertion of uncalibrated sensors as part of these embedded sensors can continuously generate responses for authentication that are tracking the signal produced by the calibrated sensors. It becomes then possible to authenticate each smart phone by their PUF sensor for the purpose of digital right managements, anti-theft, and software protection.

[0052] ***Example #4: Protection of medical devices***. Connecting medical devices, such as a pace maker, to a network of medical devices, is potentially desirable, as long as malicious entities are prevented from interacting with the medical devices. For this type of application it is important for the medical devices to authenticate a valid network. Often medical devices have embedded sensors to measure physiological parameters such as blood pressure, heart rate, or blood composition. A differential PUF system based on some of these sensors can block a communication with the network if a proper challenge is not provided during authentication.

[0053] ***Non-linear operations and multi-challenges***. The response of most sensors stops to provide responses proportional to a physical or chemical signal when these signals are outside a linear region, either at very small values, or on the other extreme, at very high values. This operating mode is called non-linear. In the non-linear region both sensors might not track each other and the hamming distance could vary significantly with the magnitude of the physical or chemical signals. This offers opportunities to create stronger cryptographic protocols. One method is to capture several hamming distances for a particular closed loop system measured with different magnitudes of physical or chemical signals. The same sensor system can thereby be described by a set of challenges rather than a single challenge which can strengthen the authentication process considering that multiple responses will be needed. A similar structure can be applied for open loop architectures, multiple known physical or chemical signals are then needed for authentication. The following two examples are presented to better explain how the non-linear operation can be exploited to strengthen the trustworthiness of the system.

[0054] ***Example #5: User authentication***. Reusing the setup described above in example #2, the transmitter may send three known magnetic fields at three different magnitudes. Access is granted if the three responses can match with the corresponding challenges.

[0055] ***Example #6: Protection of medical devices***. Building on example #4, the differential sensors can be characterized upfront with two levels of blood pressure measurements, to generate two challenges. This can enhance security and reduce false negative authentications.

[0056] **Block diagram of a closed loop system**.

[0057] In Fig. 10 a simplified block diagram of a differential PUF generator and a cryptographic protocol is shown. The signal produced by the sensing reference is processed by the analog to digital circuit (A/D) and a calibration table. The PUF sensing signal is processed the same way without calibration. The PUF generator can “XOR” both signals to produce challenges and responses. For cost reduction purposes both sensors can share the same A/D circuitry and digital processing. The cryptographic protocol may be similar to one previously presented and may include a communication with a secure server that can store the challenges and perform the authentication. It has to be noted that most sensor systems are full “system-on-chip” (SOC) devices. The percentage of the die area of the SOC that is the sensing element is very small compared with the size of the A/D and digital signal processor. Adding a second sensor to the SOC to provide PUF functionality may have a minor impact on the overall size of the SOC, thereby only a small impact on the cost structure. The bloc diagram shown in Fig. 10 can be integrated in a monolithic SOC with die size not much bigger than a SOC with a single sensor.

[0058] ***Combination.*** The methods describing the use of calibration tables and the methods describing the use of differential sensors may be combined in multi-PUFs architecture. For example CRPs can be generated from the calibration table of the reference sensor shown Fig. 9 and additional CRPs can be generated from the differential architecture.

[0059] Additional Embodiments

[0060] Streams of data, the PUF challenges and PUF responses are generated from calibration tables that are stored in sensor systems. Each sensor is thereby described by a particular PUF challenge that needs to be matched with the corresponding PUF response during an authentication cycle.

[0061] In one embodiment, the PUF generator may exploit the entire calibration table, or a portion of the calibration table, as specifically described by a set of instructions.

[0062] In another embodiment, a PUF generator may generate PUF challenges and responses by combining previously described methods together with other PUF generators based on, not to be limited to, other sensor PUFs, embedded SRAMs, non-volatile embedded memories, ring oscillators, or gate delays.

[0063] In another embodiment, un-calibrated sensors paired with calibrated sensors may be used to generate PUF parameters. The hamming distances between the two sensors generate the challenges and the responses. Each sensor is described by a particular PUF challenge that needs to be matched with the corresponding PUF response during an authentication cycle.

[0064] In another embodiment, the PUF sensors previously described may generate one challenge to be matched with one response, or multiple challenges to be matched with multiple corresponding responses.

[0065] In another embodiment, the sensors previously described may be operated in their linear range where the electrical signal produced by the sensor is proportional with the input signal that was produced by a physical or chemical parameter.

[0066] In another embodiment, the sensors previously described may be operated in their non-linear range where the electrical signal produced by the sensor is not proportional with the input signal that was produced by a physical or chemical parameter.

[0067] In another embodiment, the PUFs based on calibration tables may be combined with the PUFs based on an un-calibrated sensor paired with a calibrated sensor to form a multiple PUF system.

[0068] In another embodiment, the sensors previously described may be accelerometers, gyroscopes, magnetometers, image sensors, chemical sensors, biological sensors, medical sensors, and/or pressure sensors.

[0069] In another embodiment, the application that incorporate the sensors previously described is related to the smart grid, user authentication and access control, smart phone and terminal authentication, medical device authentication and pace makers, cyber physical systems or the Internet of things.

[0070] Other embodiments and uses of the above inventions will be apparent to those having ordinary skill in the art upon consideration of the specification and practice of the invention disclosed herein. It should be understood that features listed and described in one embodiment may be used in other embodiments unless specifically stated otherwise. The specification and examples given should be considered exemplary only, and it is contemplated that the appended claims will cover any other such embodiments or modifications as fall within the true scope of the invention.

CLAIMS

The invention claimed is:

1. A method comprising the steps of:

measuring and storing by a sensor system a calibration table for a sensing element in a non-volatile memory of the sensor system, wherein the calibration table comprises a plurality of PUF responses;

receiving from the sensor system and storing by a secure server the calibration table in a non-volatile memory of the secure server, wherein the calibration table comprises a plurality of PUF challenges corresponding to the plurality of PUF responses;

receiving from the sensor system by the secure server, a PUF response in the plurality of PUF responses; and

upon matching, by the secure server, the PUF response with a corresponding PUF challenge in the plurality of PUF challenges, authenticating the sensor system.

2. The method of claim 1, wherein the sensor system comprises a physically unclonable function.

3. The method of claim 2, further comprising the step of performing an additional physically unclonable function for authentication to form a multiple PUF system.

4. The method of claim 1, wherein the sensor system is configured to measure a physical or chemical parameter.

5. The method of claim 1, wherein the matching comprises statistically matching.

6. The method of claim 1, wherein the calibration table comprises a plurality of addresses and a corresponding plurality of calibration data and wherein at least one PUF response in the plurality of PUF responses comprises calibration data from at least two different addresses in the plurality of addresses.

7. A method comprising the steps of:

measuring by a sensor system a hamming distance for a known signal between a PUF sensor without calibration and a reference sensor with calibration;

receiving from the sensor system and storing by a secure server the hamming distance in a non-volatile memory of the secure server, wherein the hamming distance comprises a PUF challenge;

applying the known signal to the PUF sensor and the reference sensor of the sensor system;

receiving by the secure server a PUF response from the sensor system; and

upon matching by the secure server the PUF response with the PUF challenge, authenticating the sensor system.

8. The method of claim 7, wherein the sensor system comprises a physically unclonable function.

9. The method of claim 8, further comprising the step of performing an additional physically unclonable function for authentication to form a multiple PUF system.

10. The method of claim 7, wherein the sensor system is configured to measure a physical or chemical parameter.

11. The method of claim 7, wherein the matching comprises statistically matching.

12. The method of claim 7, wherein the known signal is in a linear range of the sensor system.

13. The method of claim 7, wherein the known signal is in a non-linear range of the sensor system.

14. A method comprising the steps of:

measuring by a sensor system a first hamming distance for a first known signal and a second hamming distance for a second known signal between a PUF sensor without calibration and a reference sensor with calibration;

receiving from the sensor system and storing by a secure server the first hamming distance and the second hamming distance in a non-volatile memory of the secure server, wherein the first hamming distance comprises a first PUF challenge and the second hamming distance comprises a second PUF challenge;

applying the first known signal to the PUF sensor and the reference sensor of the sensor system;

receiving from the sensor system by the secure server a first PUF response;

applying the second know signal to the PUF sensor and the reference sensor of the sensor system;

receiving from the sensor system by the secure server a second PUF response; and

upon matching, by the secure server, the first PUF response with the first PUF challenge and the second PUF response with the second PUF challenge, authenticating the sensor system.

15. The method of claim 14, wherein the sensor system comprises a physically unclonable function.

16. The method of claim 15, further comprising the step of performing an additional physically unclonable function for authentication to form a multiple PUF system.

17. The method of claim 14, wherein the sensor system is configured to measure a physical or chemical parameter.

18. The method of claim 14, wherein the matching comprises statistically matching.

19. The method of claim 14, wherein the first known signal is in a linear range of the sensor system and the second known signal is in a non-linear range of the sensor system.

20. The method of claim 14, wherein the first known signal and the second known signal are in a non-linear range of the sensor system.

ABSTRACT

Sensors convert physical and/or chemical signals into electric signals driving microelectronic systems. In order to generate electric signals that accurately represent the physical or chemical signals, calibration techniques have to compensate for the natural variations which are created during the manufacturing process of the sensors. Several methods may be used to exploit the natural physical variations of sensors, to generate cryptographic physically unclonable functions (PUF) that may strengthen the cybersecurity of microelectronic systems. One method comprises extracting a stream of bits from the calibration table of each sensor to generate reference patterns, called PUF challenges, which can be stored in secure servers. The authentication of the sensor is positive when the data streams that are generated on demand, called PUF responses, match the challenges. To prevent a malicious party from generating responses, instructions may be added as part of the PUF challenges to define which parts of the calibration tables are to be used for response generation and what additional responses may be generated by the embedded RAMs. Another method is based on differential sensors, one of them having the calibration module disconnected. The response to a physical or chemical signal of such a sensor may then be used to authenticate a specific pair of sensor.

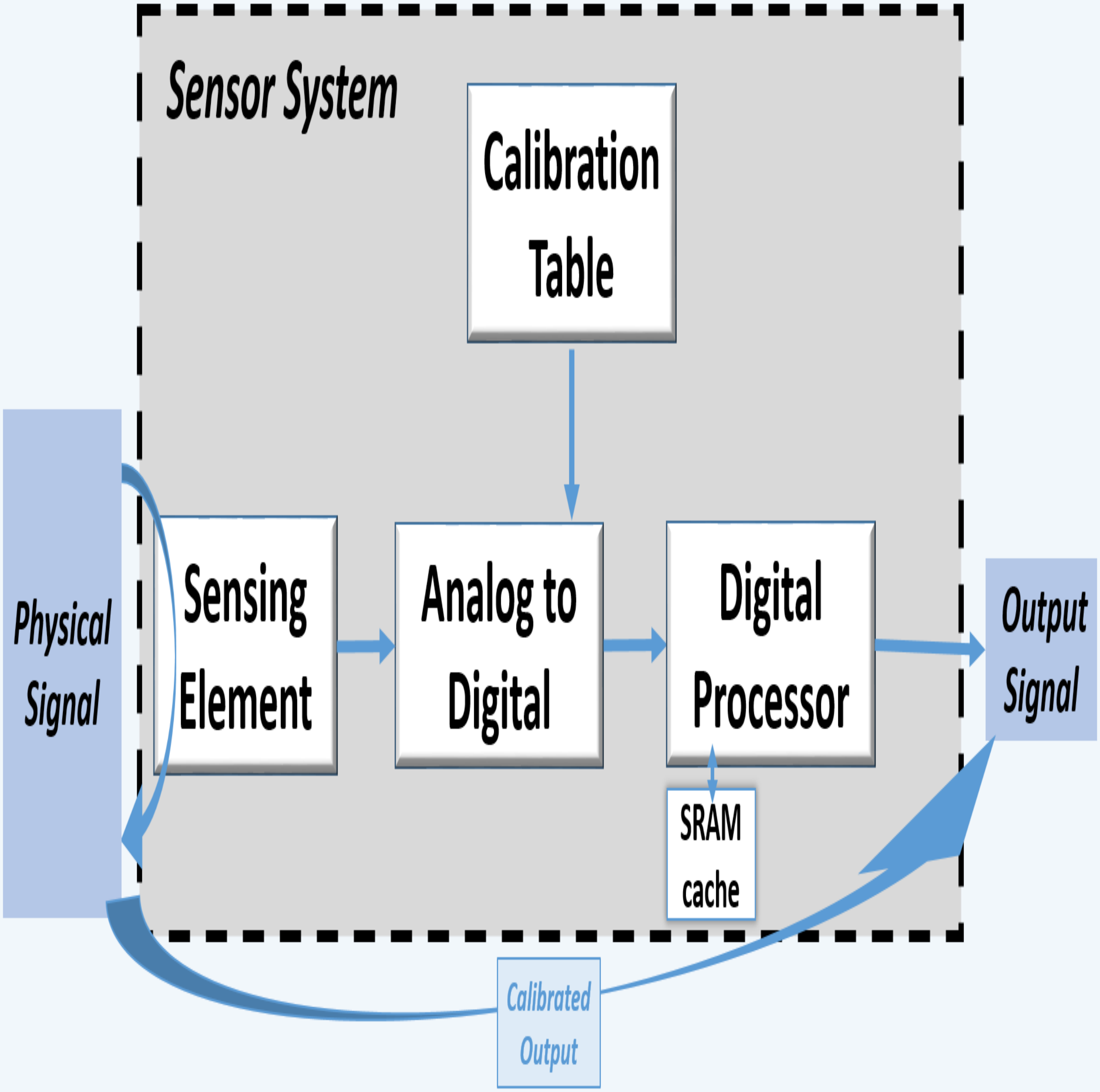

Fig.1: Block diagram of a sensor system

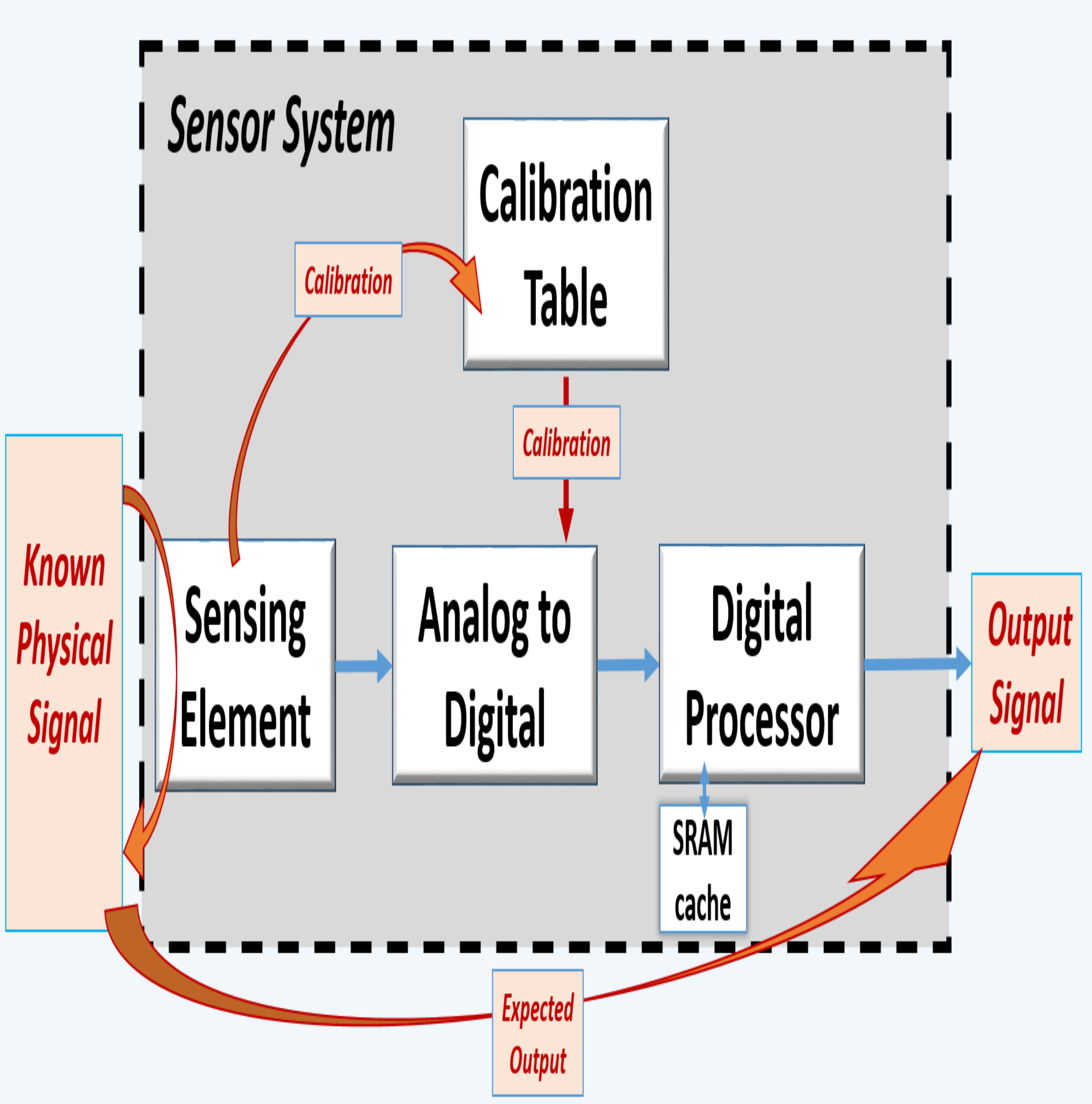

Fig.2: Calibration of a sensor system

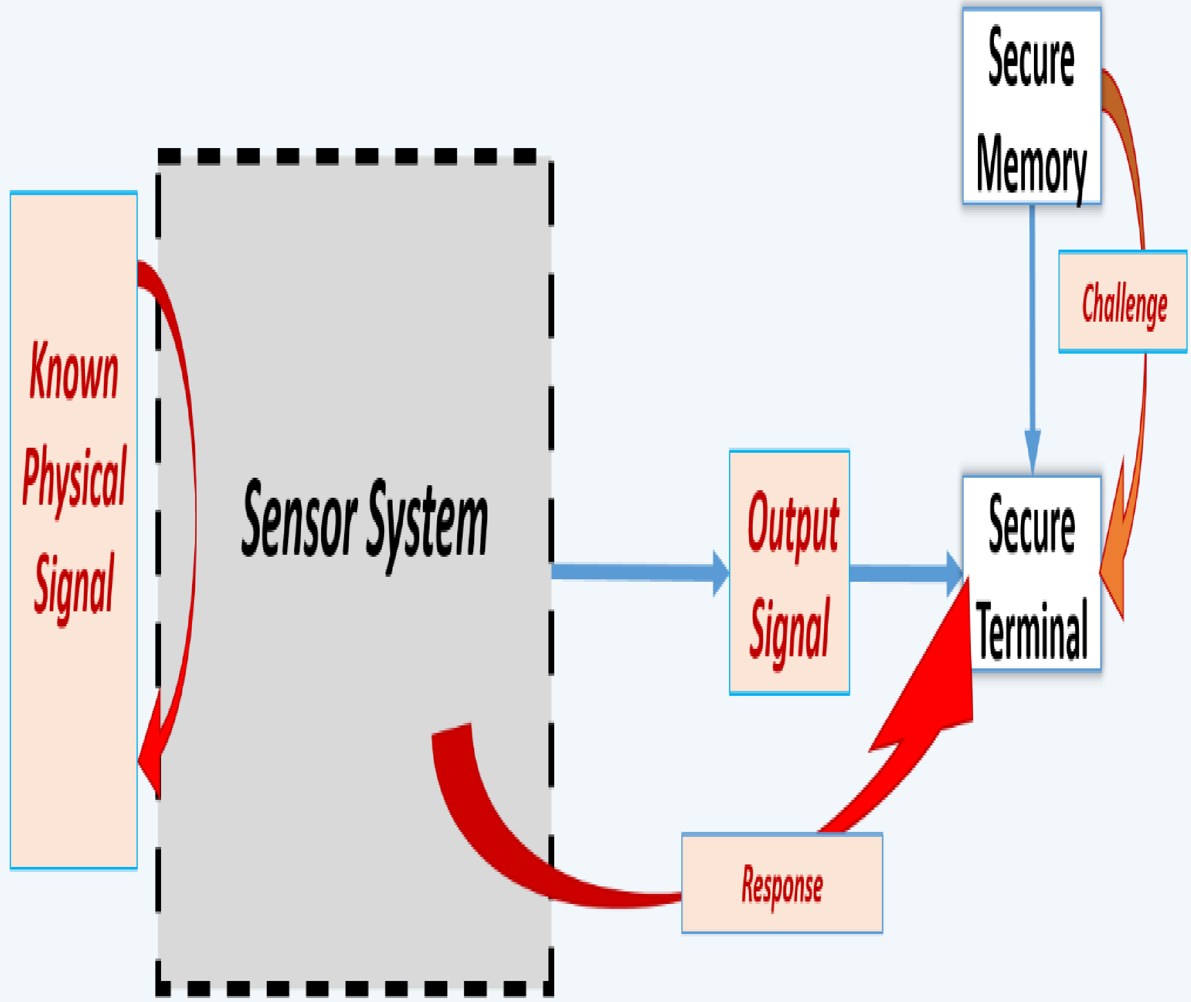

Fig.3: prior art> sensor PUF

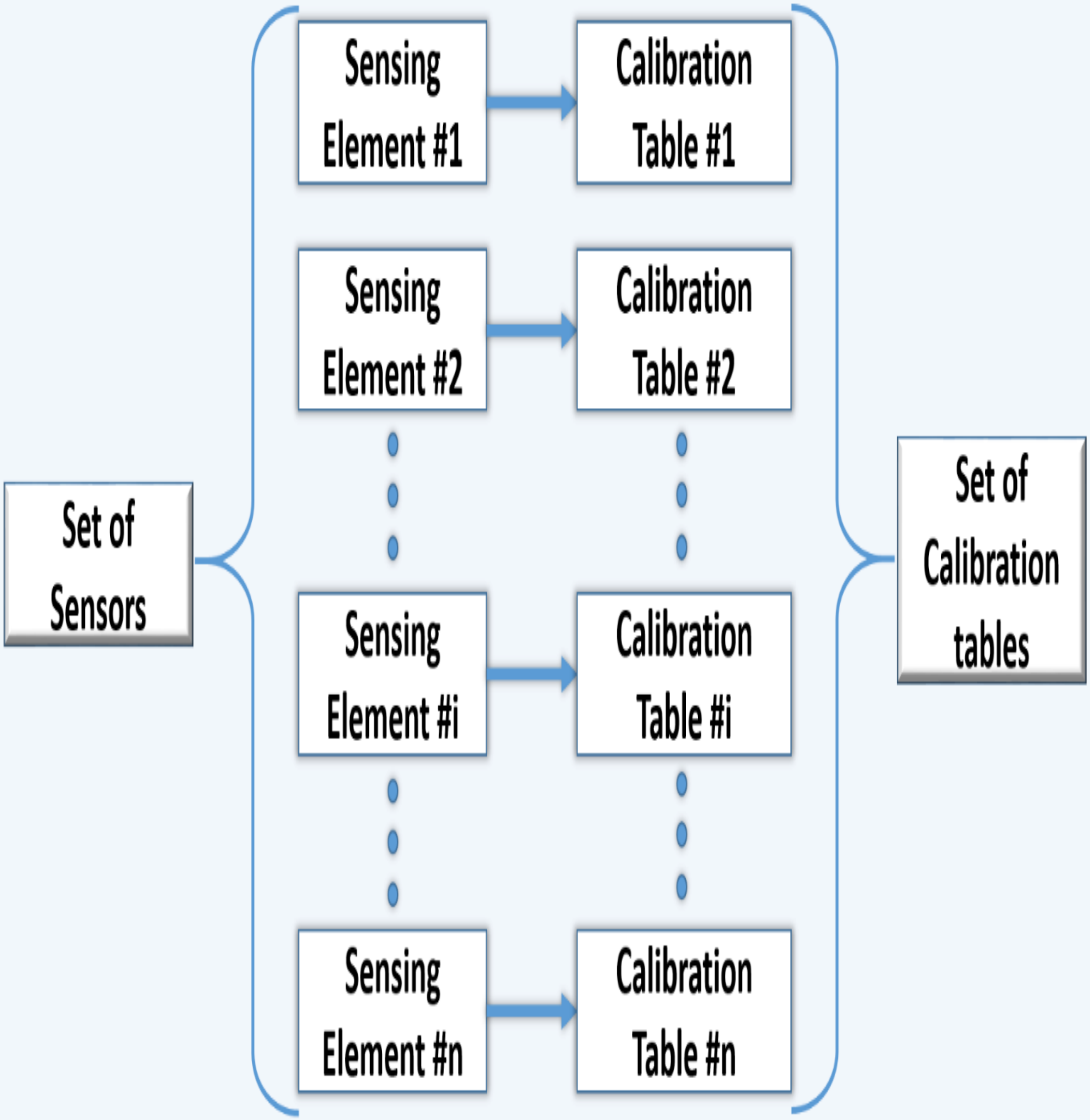

Fig.4: Set of calibration tables

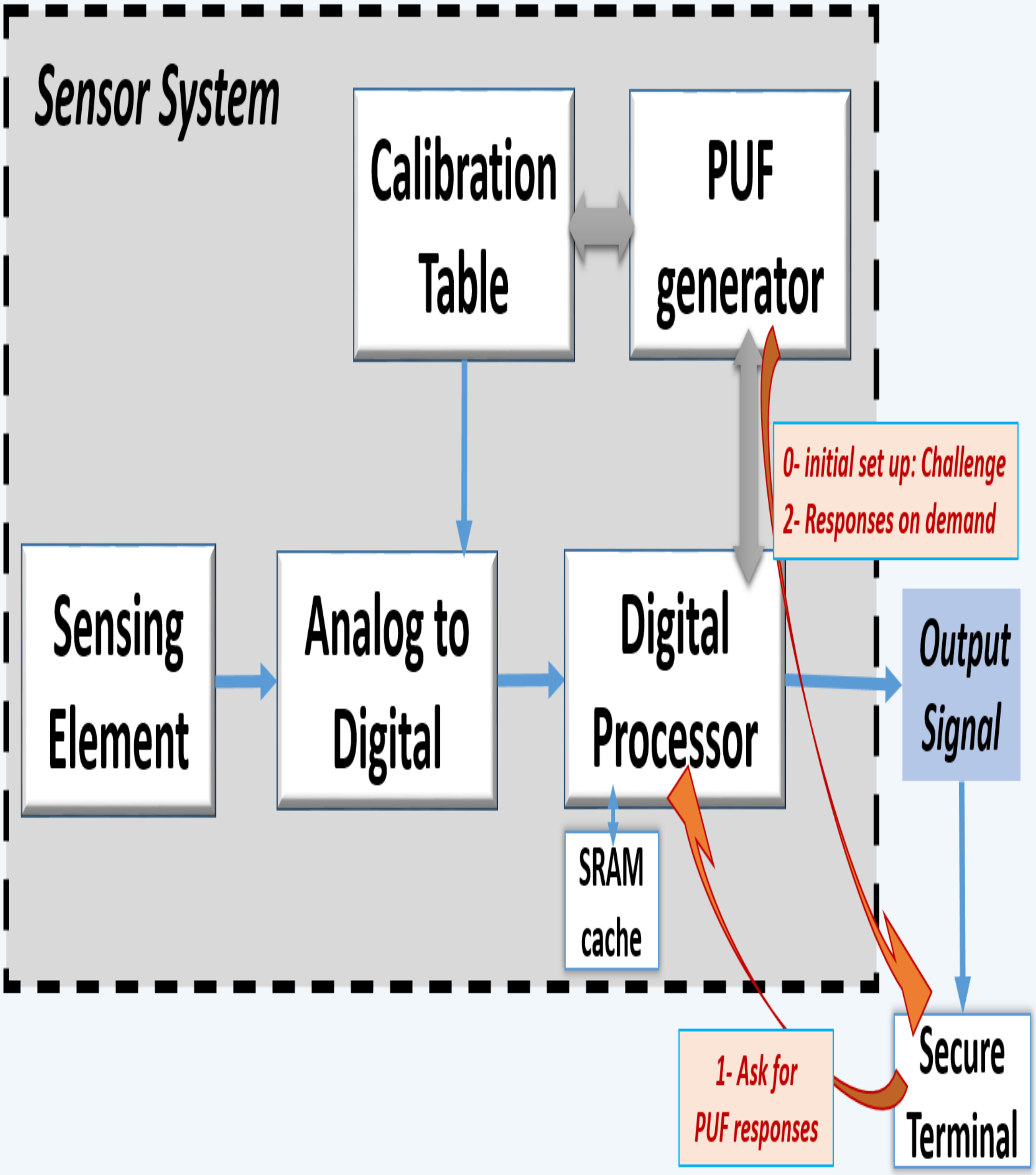

Fig.5: PUF generator based on calibration tables

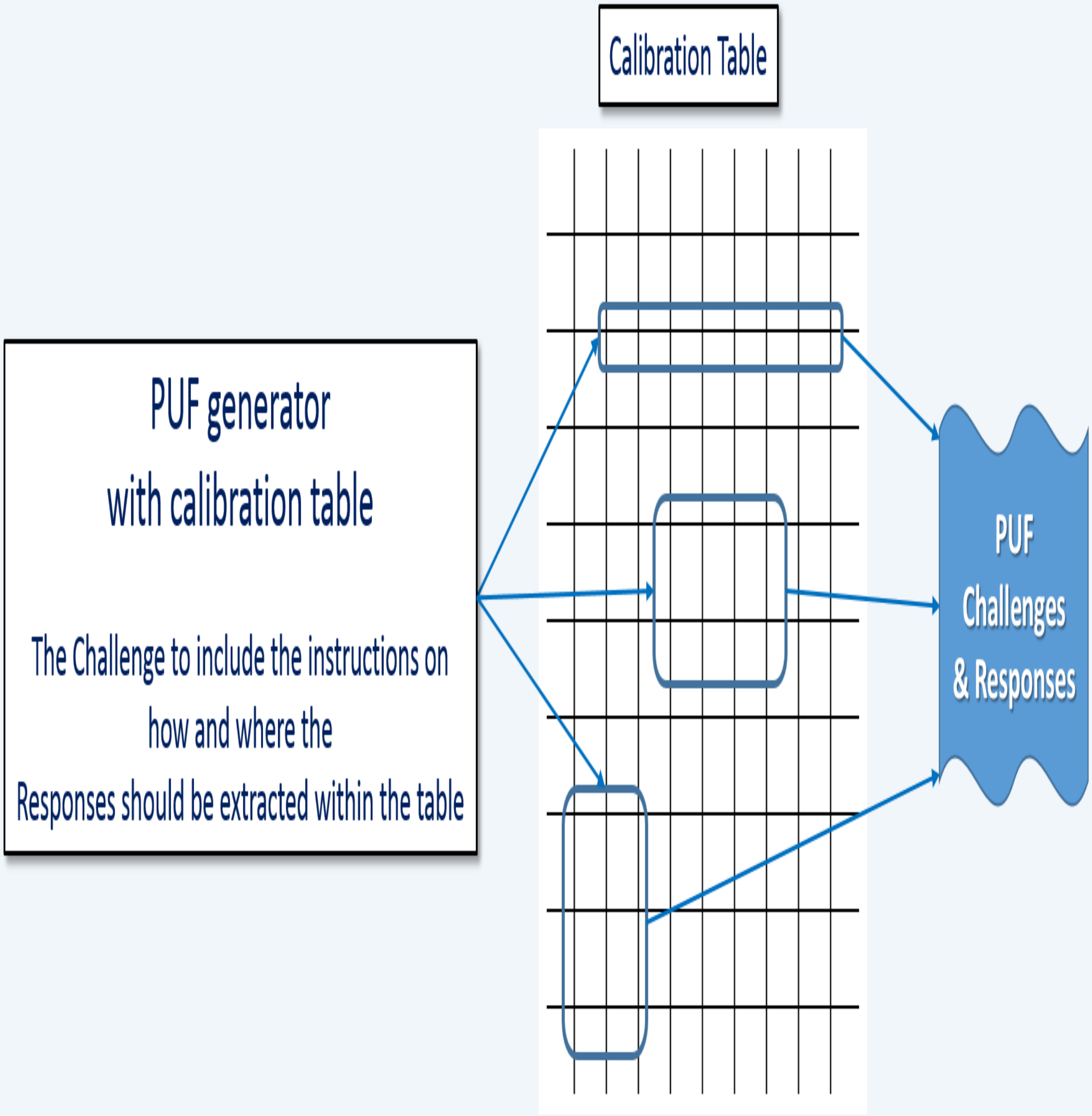

Fig.6: Hiding the location of the PUF generation within calibration table

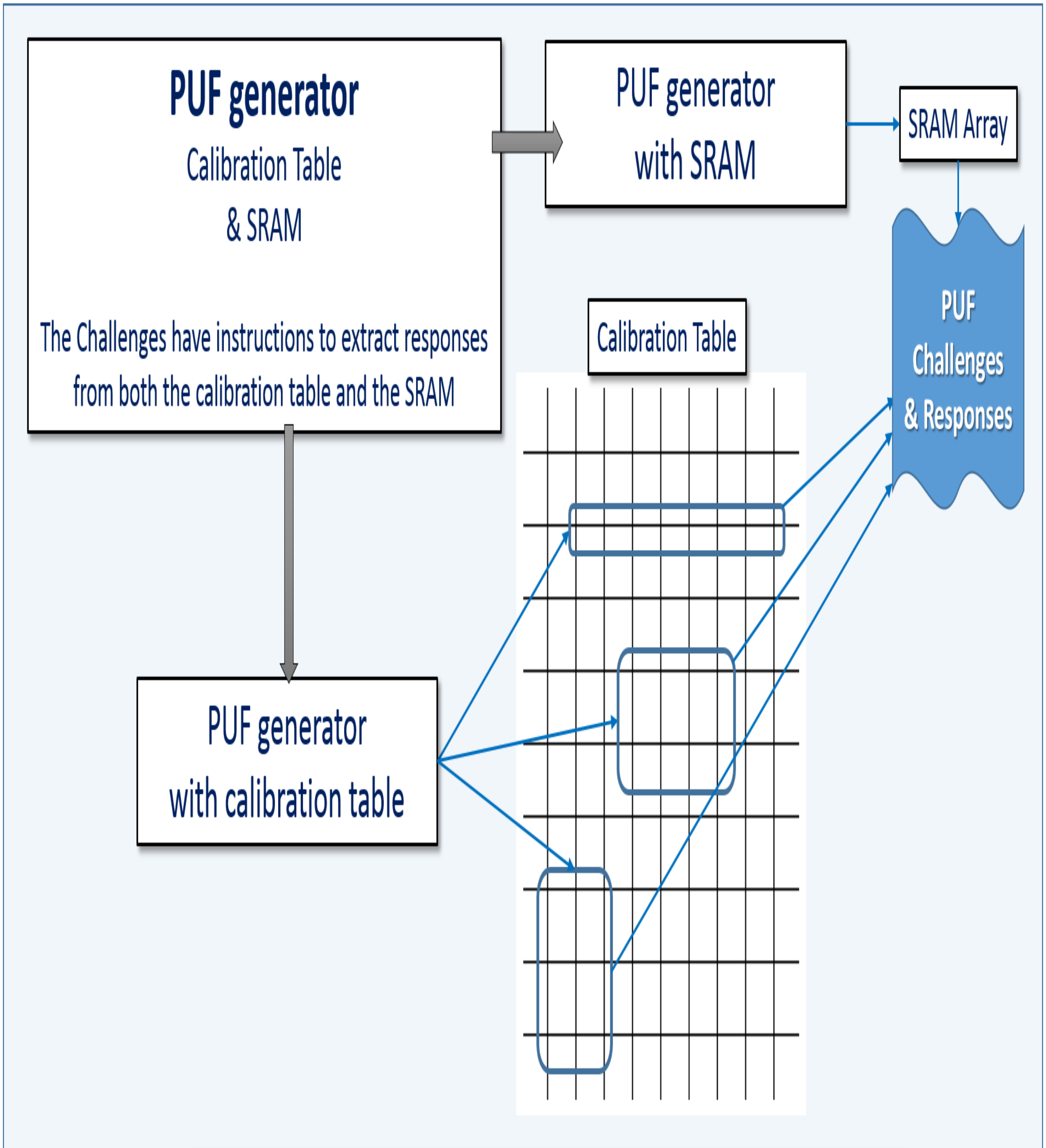

Fig.7: PUF generation with calibration table & SRAM

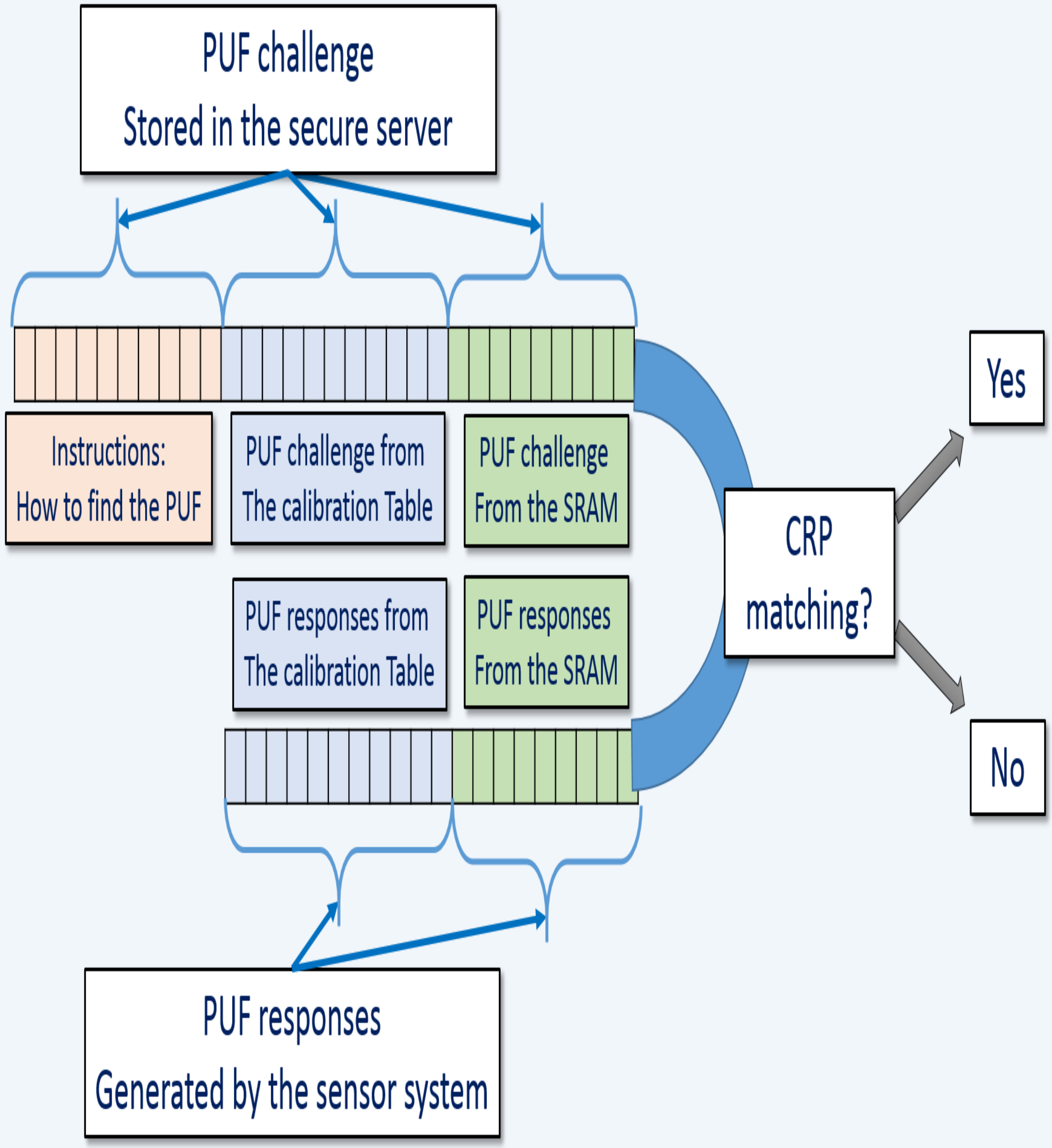

Fig.8: PUF generation: example of challenge-response-pair matching

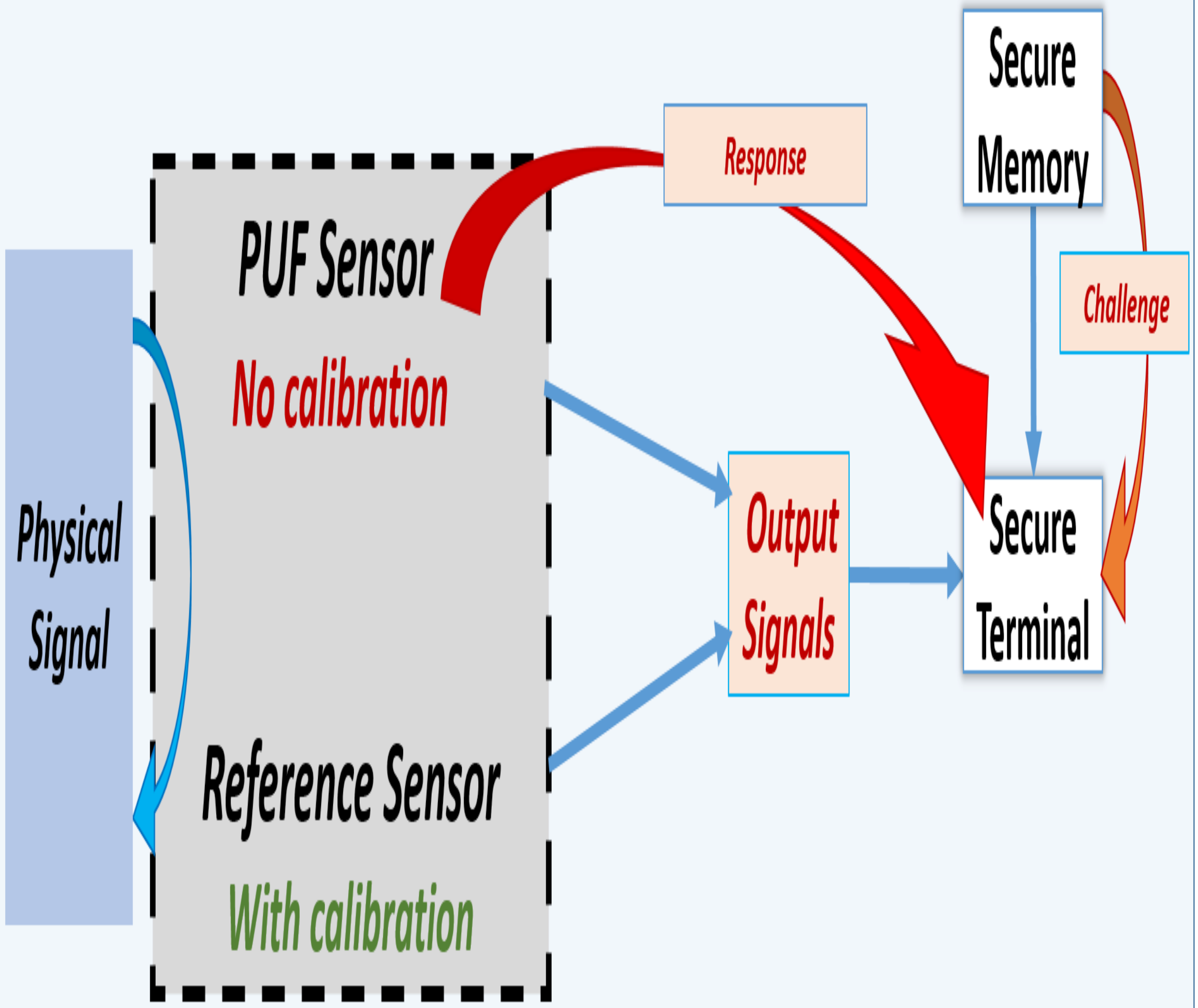

Fig.9: Differential PUF generator

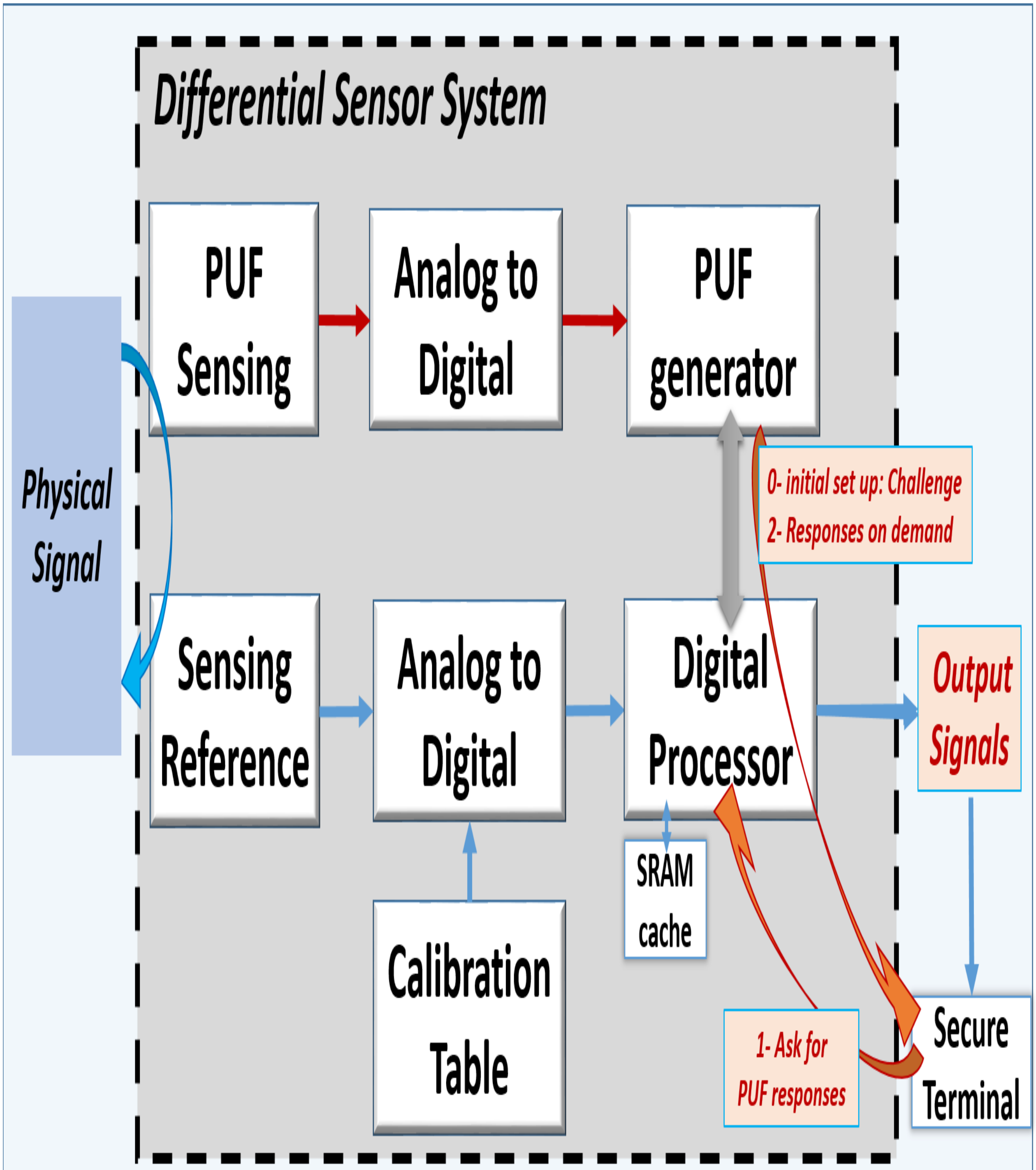

Fig.10: Differential PUF generator- signal processing