applied sciences

MDPI

Article

New Security Improvements in Next-Generation Passive Optical Networks Stage 2 †

Vlastimil Clupek [1,2,*,‡], Tomas Horvath [1,3,‡], Petr Munster [1,3,‡] and Vaclav Oujezsky [1,‡]

1 Department of Telecommunication, Brno University of Technology, Technicka 12, 616 00 Brno, Czech Republic; horvath@feec.vutbr.cz (T.H.); munster@feec.vutbr.cz (P.M.); oujezsky@feec.vutbr.cz (V.O.)
2 IT4Innovations, VSB–Technical University of Ostrava, 17. listopadu 15/2175, 708 33 Ostrava-Poruba, Czech Republic
3 Department of Optical Networks, CESNET a.l.e., Zikova 4, 160 00 Prague, Czech Republic
* Correspondence: clupek@feec.vutbr.cz; Tel.: +420-541-146-954
† This paper is an extended version of our paper published in 2019 42nd International Conference on Telecommunications and Signal Processing (TSP).
‡ These authors contributed equally to this work.

Received: 16 September 2019; Accepted: 15 October 2019; Published: 18 October 2019

Abstract: Passive optical networks are currently the most promising solution for access networks. These networks rely on broadcast signal distribution in the downstream direction and unicast signal transmission in the upstream direction. The upstream direction is controlled by optical line termination (OLT). The broadcast transmission method increases security vulnerability because the attacker is able to connect his/her modified optical network unit (ONU) to the free port of the splitter (commonly in the basement). We present the concept for the activation process of ONUs based on physical unclonable function (PUF) for next-generation passive optical networks stage 2 (NG-PON2). The use of PUF increases security in the NG-PON2. Furthermore, the registration identifier (ID) is not stored in a nonvolatile memory, in comparison with the common solution defined by the International Telecommunication Union (ITU) recommendation G.989.3. An attacker cannot perform a reverse engineering attack to obtain the registration ID. For this reason, the attacker cannot clone an ONU. We proposed security improvements that involve authentication, encryption, integrity protection, and data origin verification methods in the NG-PON2. Our model uses the standard implementation of the transmission convergence layer of NG-PON2 with the new physical layer operations, administration, and maintenance (PLOAM) messages. The recommendation G.989.3 allows specifying own PLOAM messages since not all IDs are used in the current specification.

Keywords: NG-PON2; physical unclonable function; transmission convergence layer; PLOAM messages; security

1. Introduction

Network operators continue to witness an exponential growth of traffic transmitted over their infrastructure/networks. Increasing the bandwidth means bringing an optical fiber from the edge point closer to the access part of their networks. Bringing fiber closer to customers requires the proper installation and standardized technology. Installation works are able to provide the companies, but the standardized technologies are part of network operator members of the full service access network (FSAN) that cooperates on the definition of their requirements for new passive optical network (PON) technologies [1].

Currently, the gigabit PON (GPON) specification of PON is widely used around the world [2]. However, this technology is approximately 10 years old, and the price of active elements, such as the

optical line termination (OLT) and optical network unit (ONU), and its compatibility with the older standard indicate that next-generation (symmetric) PON (XG(S)-PON) will have a larger revenue in 2021 in comparison with GPON [3]. It also proves that the speed of PON is not the most important aspect [4,5]. The next-generation PON stage 2 (NG-PON2) currently operates as a pilot project; on the other hand, the first specification of NG-PON2 was approved in 2015, which serves to illustrate the path from standardization to real deployment.

NG-PON2 networks are the first to support up to 8 wavelengths in the downstream and upstream direction. The end unit selects the proper wavelength in the activation process once it has been turned on for the first time or restarted or by the physical layer operations, administration, and maintenance (PLOAM) control message. The specification of the physical layer, such as attenuation classes, the split ratio, etc., can be found in [6]. NG-PON2, as well as all other PONs in the downstream direction, are broadcast to all ONU at the ODN, and the upstream direction uses the time division multiplex (TDM) technique with time slots.

The NG-PON2 standard must ensure protection against the following threats.

- As downstream data in NG-PON2 are broadcast to all ONUs attached to the NG-PON2 OLT channel termination (OLT CT) [7], it is necessary to ensure that a malicious user would not be capable of replacing or reprogramming an ONU to receive all downstream data intended for all connected users.
- As upstream data received by the OLT CT can originate from any ONU attached to the optical distribution network (ODN) [7], it is necessary to ensure that a malicious user would not be capable of replacing or reprogramming an ONU and forge frames to impersonate a different ONU.
- Furthermore, it is necessary to ensure that an attacker could not connect to a malicious device at various points of the infrastructure that could intercept and/or generate traffic and could impersonate an OLT CT or an ONU.
- It is also necessary to ensure that an attacker could not perform the replay attack and bit-flipping attack. The replay attack represents a situation when the attacker records frames transmitted on the PON and replays them back onto the PON later. The bit-flipping attack represents a situation when the attacker changes packets transmitted on the PON.

If we want to ensure the above-mentioned protection in NG-PON2, we must use cryptographic algorithms for this purpose. The most important terms in cryptographic security are authentication, confidentiality, integrity, and nonrepudiation. Authentication protocols can be used to verify the authenticity of communicating entities. Unilateral or mutual authentication can be carried out between communicating entities. The first entity is authenticated to the second entity or vice versa in the case of unilateral authentication. Both entities are authenticated to each other in the case of mutual authentication. Confidentiality ensures that only authorized entities can know classified information. Confidentiality can be ensured by encryption algorithms. Authentication and confidentiality can be performed by algorithms from symmetric or asymmetric cryptography. Asymmetric cryptography is generally more computationally and resource demanding than symmetric cryptography. Integrity ensures checking that data were not modified during the transmission between communicating entities. Integrity can be ensured by a hash function. Nonrepudiation ensures that an entity cannot deny a fact that was previously performed. Nonrepudiation can be ensured by asymmetric cryptography and symmetric cryptography using a trusted third party; see [8].

The rest of this paper is structured as follows. Section 2 introduces related works. Section 3 provides an overview of the security in NG-PON2 networks. Section 4 presents our proposal of security improvements in the NG-PON2 based on physical unclonable functions, correction codes, and robust cryptographic algorithms. Section 5 presents the security analysis of our proposal of security improvements in the NG-PON2. Finally, Section 6 concludes the paper.

2. Related Works

There are many types of PUFs that can be used in an ONU, for example, optical physical unclonable functions [9] and memory-based PUFs. Pappu [10] described an optical PUF that uses an interaction between the laser beam and the transparent optical token with an inhomogeneous microstructure to generate a speckle pattern. The disadvantage of this PUF is that it requires demanding external measurements. The output response depends on the location of the optical token, the laser orientation, and the wavelength of the laser. The authors of [11] proposed a physical unclonable function based on a single optical waveguide that they experimentally and numerically validated. The system's responses (responses of PUF) consist of speckle-like images that stem from mode-mixing and scattering events of multiple guided transverse modes [11]. This PUF again requires demanding external measurements. Grubel et al. [12] proposed a photonic PUF based on ultrafast nonlinear optical interactions in a chaotic silicon microcavity. The device is probed with a spectrally encoded ultrashort optical pulse that nonlinearly interacts with the microcavity [12]. This PUF is fast, simple, compact, and low cost. Anderson et al. developed a tamper indicating optical PUF using polyurethane adhesives with dispersed nanoparticles, where authentication is performed by the use of a wavefront-shaping controlled reflection [13]. This PUF requires demanding external measurements. There are a lot of another types of PUFs, which can be used in our security improvement. For example, the magnetoresistive random-access memory (MRAM) PUF, the dynamic random access memory (DRAM), PUF, and the memristive device based strong PUF (mrSPUF). MRAM PUF responses are generated using the unique energy-tilt, which is an outcome of the random geometric variations in the MRAM cells [14]. Their solution requires only minimal hardware and current drivers beyond conventional MRAM to supply the destabilizing current. The MRAM PUF generates a very high entropy, a low intra-distance, and a very high inter-distance. The MRAM PUF is easily constructible and evaluable and has small requirements to the area. The DRAM PUF [15,16] relies on the capacitor in the DRAM to initialize to random values at start-up time. The DRAM PUF provides a large number of input patterns (challenges) compared with other memory-based PUF circuits such as static RAM PUFs and can be used in low-cost identification applications. The mrSPUF [17] exploits the extremely large information density available in nanocrossbar architectures and the significant resistance variations of memristors. This PUF provides large challenge–response pairs (CRP—a challenge is a input for PUF and a response is an output of PUF), desirable characteristics of strong PUFs, low-cost overhead, and can be reconfigured.

There are many correction codes that can be used for the correction of PUF responses. For example, Dodis et al. proposed fuzzy extractors [18,19] to generate strong keys from biometric and other noisy data. They proposed two primitives: a fuzzy extractor that reliably extracts nearly uniform randomness R (R can be used as a key in a cryptographic application) from its input (the extraction is error-tolerant in the sense that R will be the same even if the input changes, as long as it remains reasonably close to the original) and a secure sketch that produces public information about its input w that does not reveal w and yet allows exact recovery of w given another value that is close to w [19]. The authors of [20] proposed secure and robust error correction for PUFs that uses index-based syndrome coding with an encoder and decoder. The authors of [21] presented complementary index-based syndrome (C-IBS) coding, a new and flexible fuzzy embedder for PUFs. C-IBS applies IBS several times to the same group of PUF outputs. The C-IBS has low implementation complexity and can be implemented in resource-constrained devices. The authors of [22] proposed error correction for PUFs using generalized concatenated codes. The authors of [23] explained how methods from coding theory are applied in order to ensure reliable key reproduction. The article [23] shows how codes for key reproduction in PUFs can be constructed using Reed–Muller (RM) and Reed–Solomon (RS) codes in combination with generalized concatenated codes. The authors of [24] introduced a scheme that only uses an error correcting code without any further helper data. The main idea is to construct for each PUF instance an individual code that contains the initial PUF response as a codeword. They use low-density parity-check (LDPC) codes; however, other code classes are also possible.

We deal with the GPON security issue [25–27]. Our model is based on the propagation delay between the OLT and ONUs. Each ONU has a different distance from the OLT due to the different floors of each customer and the reserve of the optical fiber in a customer's flat or house.

The main contribution of our article is the improvement of security in the NG-PON2 by the use of PUFs, correction codes, and more suitable cryptographic algorithms. Suitable PUFs for use in the NG-PON2 are optical and memory-based PUFs. For example, the DRAM PUF is a low-cost solution suitable to implement in an ONU. The algorithm that is suitable for the encryption of the XG-PON encapsulation method (XGEM) payload and data encryption keys is the Advanced Encryption Standard cipher-based message authentication code (AES-CMAC) with a 128-bit key. The AES-CMAC mode ensures confidentiality, authenticity, and integrity of binary data. The suitable algorithm for integrity protection and data origin verification for ONU management and control interface (OMCI) messages in NG-PON2 is AES-CMAC-64. We emphasize that there must be mutual authentication between an ONU and an OLT CT.

3. Security in NG-PON2

This section details the current security situation in NG-PON2, presents the main possible security weakness which we defined in NG-PON2, and describes physical unclonable functions, which solve this problem.

3.1. Current Situation in NG-PON2

The NG-PON2 ensures unilateral authentication, where the ONU is authenticated to the OLT CT, and mutual authentication, where the ONU and OLT CT are authenticated to each other. The unilateral authentication (called registration-based authentication) is mandatory for ONU devices connected to the NG-PON2. There are two authentication mechanisms that can be used for mutual authentication between the ONU and OLT CT in the NG-PON2. The first mutual authentication scheme uses the OMCI message exchange. The second mutual authentication scheme uses the Institute of Electrical and Electronics Engineers (IEEE) 802.1X message exchange. Support of mutual authentication mechanisms is mandatory for implementation at the component level, but optional from an equipment specification perspective [7]. The transmission convergence layer implementation has the capability to support both mutual authentication schemes, but the equipment may choose to support only unilateral authentication.

The above-mentioned authentication methods work with a registration_ID that is stored in an ONU. The registration_ID has length of 288 bits and is stored in nonvolatile storage in the ONU. It is necessary to ensure that the registration_ID is stored securely. If an attacker obtains the Registration_ID, it could clone the ONU. The ONU and the OLT CT calculate the master session key (MSK) and derived shared keys based on the registration_ID. After the calculation of the MSK and derived shared keys, they become active. The OLT CT and ONU discard the MSK and derived shared keys at the start of the activation cycle.

The confidentiality of a XGEM payload and the integrity of a PLOAM and OMCI messages are ensured in the NG-PON2 system. NG-PON2 uses several keys for ensuring confidentiality and integrity. The AES-CMAC [28] algorithm is used to compute the MSK and derived shared keys, which are the session key (SK); OMCI integrity key (OMCI_IK); physical layer operations, administration, and maintenance (PLOAM); integrity key (PLOAM_IK); and key encryption key (KEK). These keys have a length of 128 bits. MSK is derived from the registration_ID. SK is derived from MSK and the ONU serial number with a length of 64 bits. OMCI_IK, PLOAM_IK and KEK are derived from SK.

An XGEM payload is encrypted by the AES-128 cipher operated in the counter mode (AES-CTR) [29] in the NG-PON2. The disadvantage of this encryption method is that the integrity of the encrypted message is not ensured. The data encryption keys are transmitted between the OLT CT and the ONU in the encrypted form created by the AES-128 block cipher in an electronic codebook mode (AES-ECB) [30]. This method also does not ensure the integrity of encrypted data.

Integrity protection and data origin verification for PLOAM messages is ensured by the 8-byte message integrity check (MIC) field of the PLOAM message format. AES-CMAC-64 is used to construct the MIC field.

Integrity protection and data origin verification for the OMCI traffic is ensured by the 4-byte MIC field of the OMCI message format. AES-CMAC-32 is used to construct the MIC field.

There is no nonrepudiation of the origin or nonrepudiation of the delivery of data in NG-PON2.

3.2. Main Possible Security Weakness

Currently, cryptography is confronted by many cyberattacks. The brute force attack [31] is the simplest and oldest. An attacker tries to guess a secret key in the brute force attack. This attack may act ineffectively, but due to the development of computers, this attack was used in many cases. The increase in computer performance caused an increase in the length of authentication and encryption keys used in cryptographic algorithms. If the length of the secret key is sufficiently long and does not allow performing the brute force attack in polynomial time, an attacker can find security or implementation weaknesses of the used cryptographic algorithm for the purpose of unauthorized authentication or obtaining the secret key. Another way that the attacker can obtain the authentication and encryption key is by tampering with the device. If the attacker obtains the secret key, then it is able to use it for authentication and decrypting data. The attacker can also create a clone of the device from which the attacker obtained the secret key. This problem can also occur in NG-PON2 in the case where the attacker somehow obtains the registration_ID of an ONU. The attacker can use the registration_ID for authentication and to compute the MSK and derived shared keys. The attacker can also clone the ONU by using its registration_ID. This is the main security weakness that we observe in the NG-PON2 standard. This security threat can be solved by physical unclonable functions [32].

3.3. Physical Unclonable Functions

Physical unclonable functions (PUFs) are functions with an intrinsic random nature that use the heterogeneities and differences of physical components of a device to generate unpredictable unique responses. This response is called a fingerprint of the device. Heterogeneities and differences of physical components of the device are random, and they cannot be controlled by a manufacturing process. For this reason, PUFs cannot be cloned. PUFs represent an alternative to the classic storing of secret keys, which are stored in nonvolatile memories. In PUFs, a unique bit string is generated for a device when needed without the need to store it.

The main properties of PUFs are that they are constructible, evaluable, reproducible, unique, identifiable, physically unclonable, truly unclonable, mathematically unclonable, unpredictable, tamper evident, and one-way [33]. The first proposals to meet some properties of PUFs were defined 30 years ago; however, their authors did not call them as PUFs at that time. Pappu Srinivasa Ravikanth was the first to have systematically written about the concept of PUFs in his dissertation thesis [10], in 2001. Pappu called PUFs physical one-way functions (POWFs) in his thesis.

An input of a PUF is called a challenge and an output of a PUF is called a response. The definition $Response = PUF\,(challenge)$ describes a calculation of the PUF response. Assigning the response to the challenge is called a mapping process that results in a CRP. CRPs are stored in the secure database.

PUFs represent a certain type of true random number generator. One challenge of a PUF represents a query for a random number. The response of PUF is the random number created by a stochastic physical process.

PUFs can be used for authentication (biometric authentication schemes work similarly), generation of encryption keys, and solving an unauthorized increased production by a third party (the night-shift problem) [34]. If produced chips have implemented PUFs, the CRPs of unauthorized produced chips will not be in the database of CRPs; moreover, if they are used, authentication will be unsuccessful. PUFs can be also used as a signature scheme. A challenge represents a string of a message and

a response represents a signature of a message generated by an internal private key that cannot be programmed through a manufacturing approach.

The advantages of PUFs include a price reduction (it is not necessary safely store the Registration_ID i a nonvolatile memory in an ONU) and an increase of security (PUFs are resistant to reverse engineering). PUFs do not require a permanent repository to store an authentication or encryption key. This key can be generated when needed on the device at any time. The main disadvantage of PUFs is noise in output responses. PUFs generally generate noisy responses, and they contain a limited amount of entropy. For this reason, the generated response of a PUF cannot be used as an encryption key directly. The encryption key is constructed from the generated response using helper data. Errors in output responses of PUFs may have a random or deterministic nature. Random errors are caused by the noise of a peripheral device. Deterministic errors are caused by temperature differences around the device with a PUF, the aging of components of the device, an unstable supply voltage (even small voltage changes can affect to the PUF's behavior), or anything that causes variations in the internal components of the device. Deterministic errors cannot be accurately predicted, there is no equations, which can be describe changes in PUFs behavior caused by deterministic errors. Every deterministic error has a different effect on each PUF and changes its behavior differently. Correction codes are implemented together with PUFs for a correction of noisy output responses of PUFs in order to generate encryption keys. A disadvantage of correction codes is that they need a permanent memory. If PUFs are used for authentication of a device, an additional implementation of an appropriate correction code for correction output responses of PUFs will not be required. It uses the fact that generated responses of PUFs are sufficiently different from each other. Therefore, even if the output response of a PUF contains a greater number of errors, the device can be correctly identified. The calculation of the Hamming distance is usually used to make a decision regarding whether the received response is equal to the stored response in the database.

The initialization phase is a process whereby challenges are inserted many times on the input of the PUF, and the generated output responses together with the helper data are mapped to CRPs and stored in a database. This phase must be carried out in a secure environment (by a secure channel, where an attacker cannot eavesdrop the communication between the OLT CT and the ONU), usually after the production of a PUF. CRPs are used in the authentication phase, and CRPs and helper data are used in the key generation phase.

A verifier that has a database with CRPs sends a challenge to a device in the authentication phase. The device calculates a response from the received challenge by its PUF and sends the response to the verifier. The verifier compares the received response with its response that is stored in its database. If the Hamming distance between the received response and the stored response in the database is sufficiently small, the device will be authenticated. If the Hamming distance between the received response and stored response in the database is too large, the device will not be authenticated. A positive decision about authentication depends on the place where the intra-distance histogram and inter-distance histogram overlap. The intra-distance histogram represents the distance between the two responses that were made by one PUF by using the same single challenge (the required value of the intra-distance is equal to 0%). The inter-distance histogram represents the distance between the two responses that were made by two PUFs by using the same single challenge (The required value of the inter-distance is equal to 50%). The threshold for optimal authentication (equal error rate (EER)) is somewhere in the gap between these histograms; see Figure 1. If these histograms overlap, the device can be incorrectly identified (false acceptance rate (FAR)) or cannot be identified at all (false rejection rate (FRR)). To achieve the appropriate decision level, it is recommended to minimize the sum of the FRR and FAR. An example of an authenticated device can be a smart card (a radio frequency identification (RFID) tag), and an example of a verifier can be a smart card reader.

An entity that has a database with CRPs and helper data sends a challenge of corresponding helper data to a device in the key generation phase. The device calculates a shared key from the

received challenge and helper data by its PUF and correction code. The shared key may be used for authentication of the device or encryption of data.

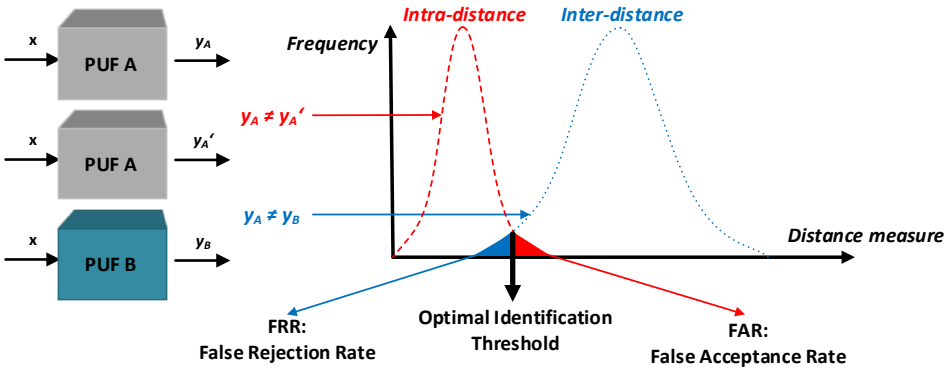

Figure 1. Intra-distance and inter-distance histogram [35].

4. Our Proposal of Security Improvements in NG-PON2

We discern four security threats in NG-PON2: The first and main security threat is that the registration_ID of an ONU is stored in nonvolatile memory in the ONU [36]. If an attacker somehow obtains the registration_ID from the ONU, it can use it for authentication, to generate the MSK and derived shared keys, and to clone the ONU. The second security threat is that the encryption algorithms AES-CTR (used for the encryption of a XGEM payload) and AES-ECB (used for the encryption of the encryption keys) do not provide integrity of the encrypted data. The third security threat is that integrity protection and data origin verification for OMCI messages are ensured by AES-CMAC-32, which enables guessing attacks. The fourth security threat is that only unilateral authentication of an ONU to an OLT CT is mandatory.

First, we introduce the NG-PON2 security improvement, which we called SI-NG-PON2. In SI-NG-PON2, ONUs and OLT CT use a Registration_ID_PUF generated as needed by a PUF from the received challenge instead of a Registration_ID stored in nonvolatile memory on the side of ONUs. The ONU uses a correction code to correct the generated response from the PUF using the received helper data.

SI-NG-PON2 enriches NG-PON2 with four additional PLOAM messages (Request_Registration_PUF, Request_Registration_PUF1, Request_Registration_PUF2, and Registration_PUF), as well as several hardware and software requirements for ONUs and OLT CT units. On the side of an ONU, a secure PUF with a correction code (CC) must be implemented. On the side of OLT CT, a generator of challenges and secured database of PUFs' CRPs and helper data (HD) for CCs must be implemented. CRPs and HD are created and stored in the OLT CT database at the time of an initialization phase that must be performed by a secure channel. The initialization phase can be performed only using the secure channel. The initialization phase can be seen in Figure 2.

An OLT CT first generates challenges using its generator. They are consequently sent to an ONU. The ONU computes the responses along with the associated helper data using the PUF and CC and sends them back to the OLT CT. The OLT CT creates CRPs and HD databases using the previously sent challenges, the received responses, and helper data from the ONU. After the initialization phase, the ONU and OLT CT are ready to unilaterally or mutually perform authentication and encrypted communications.

A challenge and the helper data are transmitted in the one Request_Registration_PUF message. If it is necessary, the challenge and helper data can be transmitted separately in the two PLOAM messages (the challenge in the Request_Registration_PUF1 and the helper data in the Request_Registration_PUF2). In this case, it will come a increase of the traffic by 48 octets (384 bits). These downstream PLOAM messages are alternatives to the Request_Registration downstream PLOAM message with ID 0x09. A response that represents the registration ID generated by the

PUF and corrected by CC (Registration_ID_PUF) is transmitted in the Registration_PUF message. This upstream PLOAM message represents an alternative to the Registration upstream PLOAM message with ID 0x02. It is impossible to calculate the Registration_ID_PUF from the challenge and helper data without using the PUF and CC implemented in the ONU.

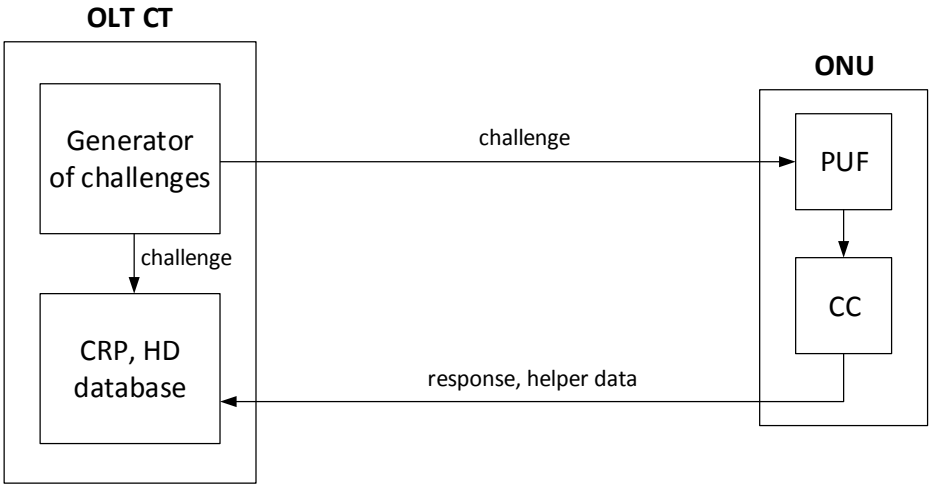

Figure 2. Initialization phase in SI-NG-PON2.

Request_Registration_PUF, Request_Registration_PUF1, and Request_Registration_PUF2 PLOAM messages, see Tables 1 and 2, serve to transmit a challenge and the helper data to the ONU. The PLOAM messages specified in Table 1 are new messages for our security improvement model. The recommendation G.989.3 defines defines the format for all messages, but the PLOAM messages implementation strongly depends on the producer of a system [7]. The mentioned document just suggests the format for interoperability for all systems. Defined messages end with 0x1C ID. Because there is one octet for ID message definition we just continued with next IDs. The Registration_PUF PLOAM message (see Tables 3 and 4) serve to transmit the Registration_ID_PUF to the OLT CT.

The content of the Request_Registration_PUF1 and Request_Registration_PUF2 message is the same as that in the Request_Registration_PUF, but in the third octet (Message type ID) is 0x1E, "Request_Registration_PUF1" for Request_Registration_PUF1, and 0x1F, "Request_Registration_PUF2" for Request_Registration_PUF2. Next, in octets 5–40, only the challenge is transmitted in the Request_Registration_PUF1 and only the helper data in the Request_Registration_PUF2 are transmitted. Unused byte positions are filled by 0x00 values. The ONU must has both the challenge and helper data in order to generate the Registration_ID_PUF.

Table 1. New downstream physical layer operations, administration, and maintenance (PLOAM) messages.

Message Type ID	Message Name (Applicability)	Function	Trigger	Effect of Receipt
0x1D	Request_ Registration_PUF (TWDM only)	To request an ONU's Registration_ID_PUF.	At the implementor's discretion; ONU has been previously activated.	Send the Registration_PUF message
0x1E	Request_ Registration_PUF1 (TWDM only)	To request an ONU's Registration_ID_PUF.	At the implementor's discretion; ONU has been previously activated.	Send the Registration_PUF message
0x1F	Request_ Registration_PUF2 (TWDM only)	To request an ONU's Registration_ID_PUF.	At the implementor's discretion; ONU has been previously activated.	Send the Registration_PUF message

Table 2. Content of Request_Registration_PUF message.

Octet	Content	Description
1–2	ONU-ID	Directed message to one ONU.
3	Message type ID	0x1D, "Request_Registration_PUF".
4	SegNo	Eight-bit unicast PLOAM sequence number.
5–40	Challenge + helper data	A string of 36 octets that combines a challenge and helper data. The challenge is separated from the helper data by the characters ‖. Unused byte positions are filled by 0x00 values.
41–48	MIC	Message integrity check computed using the default PLOAM integrity key.

Table 3. New upstream PLOAM message.

Message Type ID	Message Name (Applicability)	Function	Trigger	Effect of Receipt
0x1D	Registration _PUF (TWDM only)	To report the Registration _ID_PUF of an ONU.	When the ONU is in the Ranging state O4 (see [7]) or is responding to a ranging grant, or when the ONU is in the Operation state and is responding to the Request Registration_PUF (Registration_PUF2) message.	The OLT CT may use the ONU's Registration _ID_PUF for authentication and the generation of the MSK and derived shared keys.

Table 4. Content of Registration_PUF message.

Octet	Content	Description
1–2	ONU-ID	Directed message to one ONU.
3	Message type ID	0x1D, "Registration_PUF".
4	SegNo	Repeated from downstream Request_Registration_PUF (Request_Registration_PUF1) message, or 0 if generated in response to a ranging grant in the Ranging state (O4).
5–40	Registration_ID_PUF	A string of 36 octets that has been generated by a PUF and CC in an ONU. Registration_ID_PUF may be useful in identifying a particular ONU installed at a particular location and for a generation of the MSK and derived shared keys.
41–48	MIC	Message integrity check computed using the default PLOAM integrity key.

In the first step, the OLT CT sends a challenge and helper data to the ONU. If the ONU received a challenge and helper data, it can calculate the Registration_ID_PUF in this way. The ONU implements the received challenge as the input of PUF, and the calculated output of PUF with the received helper data is employed as the input of CC; see Equation (1).

$$Registration\_ID\_PUF = CC\left(PUF\left(challenge\right), HD\right). \quad (1)$$

In the second step, the ONU sends the Registration_ID_PUF to the OLT CT. If the OLT CT receives the Registration_ID_PUF, then it will compare the received Registration_ID_PUF with the response from its CRP database that creates the CRP pair with the challenge that the OLT CT sent to the ONU at the previous step. If they are equal, the ONU will be authenticated, and the MSK and derived shared keys can be computed by using the Registration_ID_PUF instead of the Registration_ID. The response is called Registration_ID_PUF on the ONU's side in SI-NG-PON2.

The process of the calculation and verification of the Registration_ID_PUF by an OLT CT and an ONU using the Request_Registration_PUF (Request_Registration_PUF1 and Request_Registration_PUF2) and Registration_PUF messages is shown in Figure 3.

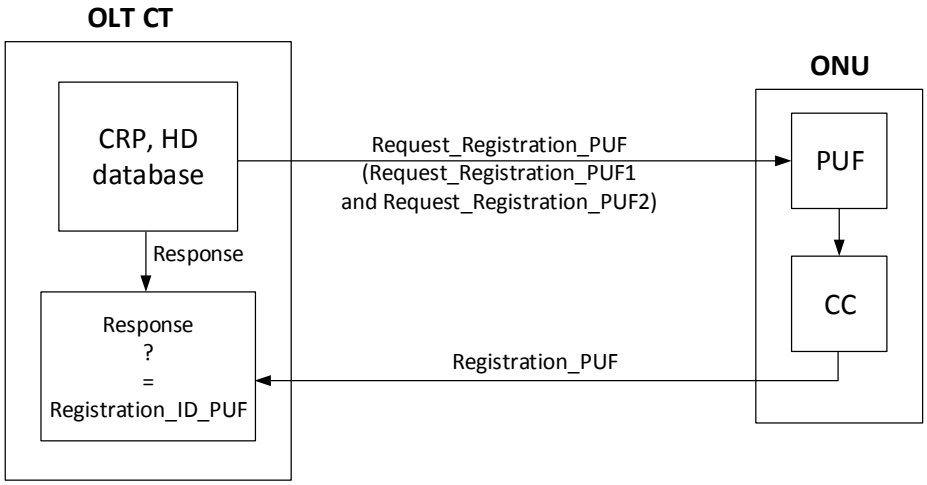

Figure 3. The process of the calculation and verification of the Registration_ID_PUF in SI-NG-PON2.

There are many PUFs and correction codes that are suitable to use in SI-NG-PON2. We propose using optical PUFs or memory-based PUFs. For example, a photonic PUF [12] is fast, simple, compact, and low-cost, or a DRAM PUF can provide a large number of input challenges and can be used in low-cost identification applications. Next, we propose to use fuzzy extractors [18,19] for correction of the PUF response or the error correction code [24], which works without any further helper data. In this case, the Request_Registration_PUF message in octets 5–40 contains only the challenge without the helper data. Unused byte positions (originally intended for helper data) are filled by 0×00 values.

Another security threat we recognize in using the encryption algorithms AES-CTR and AES-ECB in NG-PON2 is that these algorithms not provide integrity of the encrypted data. AES-CTR is used for encryption of an XGEM payload, and AES-ECB is used for encryption of the data encryption keys. If an attacker changes the transmitted encrypted XGEM payload or the encrypted data encryption keys (conducts a bit-flipping attack), the receiver cannot recognize the changed data. There are several modes for block ciphers that ensure confidentiality, authenticity and integrity of binary data, for example, the Galois counter mode (GCM) [37], cipher block chaining–message authentication code (CCM) [38], EAX [39], offset codebook (OCB) [40], and the CMAC [28]. We recommend the AES-CMAC algorithm with a 128-bit key for encryption of an XGEM payload and the data encryption keys in NG-PON2.

The next security threat we evaluate in using the AES-CMAC-32 algorithm for integrity protection and data origin verification for OMCI messages in NG-PON2 involves the following, according to [41], at least a 64-bit MAC should be used for protection against guessing attacks. The AES-CMAC-64 algorithm is used for integrity protection and data origin verification of PLOAM messages. We propose to also use the AES-CMAC-64 algorithm for integrity protection and data origin verification for OMCI messages to increase security in NG-PON2.

The last security threat we discern is the possibility of using only unilateral authentication when an ONU is authenticated to an OLT CT in NG-PON2. In this case, an attacker could connect a malicious

device to the infrastructure and could impersonate an OLT CT. Subsequently, the malicious OLT CT can acquire data from an ONU. We propose the mandatory use of mutual authentication between an ONU and an OLT CT in NG-PON2. If mutual authentication is not performed between an ONU and an OLT CT, the ONU will not further respond to the nonauthenticated OLT CT.

5. Security Analysis of Our Proposal of Security Improvements in the NG-PON2

Our security improvement SI-NG-PON2 is based on implementing a PUF with a correction code. As the secret information Registration_ID_PUF (used for authentication and generation of the MSK and derived shared keys) is not stored in nonvolatile memory in an ONU, but is instead generated as needed by using the received challenge and helper data, an attacker cannot copy this secret information from the ONU to an another device. A challenge and helper data do not reveal any information about the generated response by the PUF and CC. For these reasons, the attacker cannot clone an ONU, cannot act as another ONU and cannot decrypt an encrypted communication.

A malicious user is not able to replace or reprogram an ONU for receiving all downstream data intended for all connected users since he does not know their secret information (Registration_ID_PUF) and there is no way to calculate it without the PUF and CC implemented in the ONU. For the same reason, a malicious user is not able to replace or reprogram an ONU and forge packets (upstream data) to impersonate a different ONU.

The bit-flipping attack is not possible, as we use the AES-CMAC algorithm with a 128-bit key for encryption of the XGEM payloads and data encryption keys in our proposal of security improvement. Next, we use AES-CMAC-64 for integrity protection and data origin verification of PLOAM and OMCI messages in our proposal of security improvement. The CMAC encryption mode ensures confidentiality, authenticity and integrity of binary data. If the attacker changes some transmitted data (performs a bit-flipping attack), the subsequent check will reveal this change.

The guessing attack to integrity protection and data origin verification of OMCI messages is not possible since we use the AES-CMAC-64 algorithm. The 64-bits length of a key is enough to satisfy the protection against the guessing attack.

If an attacker connects a malicious device at various points in the infrastructure that could intercept and/or generate traffic, the malicious device will could not impersonate an OLT CT, as the mutual authentication between an OLT CT and an ONU is mandatory in our proposal of security improvement in NG-PON2. A new connected malicious device could not impersonate an ONU since an OLT CT does not have challenge–response pairs of the connected malicious device in its CRP database.

Figure 4 describes a situation when an attacker comes between an OLT CT and an ONU, and, due our security improvements cannot perform the cloning attack, bit-flipping attack, guessing attack, and impersonation attack.

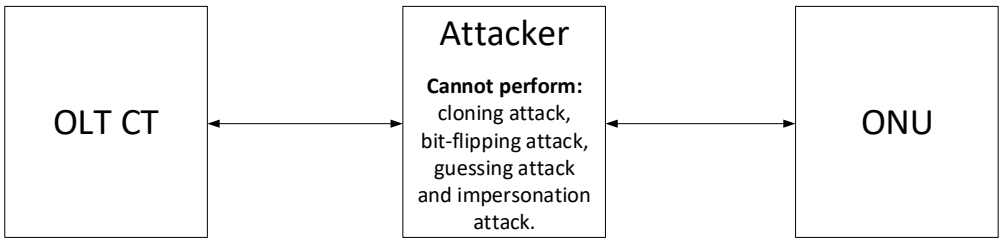

Figure 4. Unfeasible attacks on optical network unit (ONU) and optical line termination (OLT) channel termination (CT) in our security improvements.

Our security improvement (SI-NG-PON2) is based on the using PUFs in ONUs. The main condition which must be carried out in order the using of a PUF was safely is that the intra-distance of the PUF approaches 0.00% and the inter-distance of the PUF approaches 50.00%. Equations (2) and (3) show a mathematical expression of the intra-distance and inter-distance calculation [42].

$$D_{puf_i}^{\text{intra}}(x) \stackrel{\Delta}{=} dist[Y_i(x); Y_i^{'}(x)], \tag{2}$$

where $Y_i(x); Y_i^{'}(x)$ are two different and random evaluations (responses) of the one same PUF instance, puf_i, for one the same challenge x.

$$D_{C}^{\text{inter}}(x) \stackrel{\Delta}{=} dist[Y(x); Y^{'}(x)], \tag{3}$$

where C is a class of the PUF and $Y(x); Y^{'}(x)$ are two different and random evaluations (responses) for one the same challenge x by two random and different PUF instances.

We recommend a using strong PUFs in SI-NG-PON2. Since strong PUFs have a huge number of challenge–response pairs, an ONU may change Registration_ID_PUF many times during a service life of a PUF. For example, in [42] the authors presented a strong silicon PUF with 2^{65} challenge–response pairs, which is immune to machine learning's attacks.

In Table 5 is shown the comparison between NG-PON2 and our security improvements in selected security issues.

Table 5. Comparison between NG-PON2 and our security improvements in selected security issues.

Security Issue	NG-PON2	Our Security Improvements
Clone an ONU	**Yes**	**No**
Encryption of a XGEM payload provides integrity of data	**No** (uses AES-CTR-128)	**Yes** (uses AES-CMAC-128)
Encryption of the encryption keys provides integrity of data	**No** (uses AES-ECB-128)	**Yes** (uses AES-CMAC-128)
Integrity protection and data origin verification for OMCI messages enables a guessing attack	**Yes** (uses AES-CMAC-32)	**No** (uses AES-CMAC-64)
Mutual authentication between an ONU and an OLT CT is mandatory	**No**	**Yes**

6. Conclusions

In this article, we focused on security problems in next-generation passive optical networks stage 2. We propose four security improvements in the NG-PON2. Our security improvements use physical unclonable functions, correction codes, and robust cryptographic algorithms in the NG-PON2. The first security improvement (SI-NG-PON2) is based on PUFs and correction codes. PUFs bring a higher level of security and reduce cost. PUFs do not need a secured nonvolatile memory for storing authentication/encryption keys. These keys are generated on the fly by PUFs. For this reason, authentication/encryption keys cannot be copied from the nonvolatile memory and an attacker cannot clone a device. The disadvantage of PUFs is a noise in output responses. It is no problem in the simplest scenario, when PUFs are used only for authentication. In this case, the Hamming distance is used for a decision whether a device will be authenticated or not. In our security improvement (SI-NG-PON2) we need that PUFs will generate stable cryptographic keys. For this purpose, we use a correction code (fuzzy extractor) to make stable cryptographic keys from noisy outputs of PUFs.

The disadvantage of correction codes is that they need some additional memory space. The second security improvement ensures confidentiality and integrity for an XGEM payload and data encryption keys by AES-CMAC-128. The third security improvement ensures integrity protection and data origin verification for OMCI messages by AES-CMAC-64, which is immune against guessing attacks. The last security improvement introduces mandatory mutual authentication between an ONU and OLT CT. So an attacker cannot impersonate an OLT CT. In this article, we showed how PUFs can be implemented in the NG-PON2. We presented advantages of using PUFs in the NG-PON2. The main advantage is that an ONU cannot be cloned. Therefore, an unauthorized ONU cannot be active in the NG-PON2. Our security improvements involve authentication, encryption, integrity protection, and data origin verification methods that ensure a higher level of security in the NG-PON2.

Our security improvement SI-NG-PON2 can be compared to biometric cryptographic systems. Responses of PUFs can be compared to biometric information of a person. Just as a biometric cryptographic system must have some database of biometric information, SI-NG-PON2 must has a database of CRP and helper data. This database must handles the overload like a database with biometric information. There is a minimum latency increase in SI-NG-PON2 compared to NG-PON2. There is the same latency like in biometric cryptographic systems. The creation of a response takes roughly the same time like a take of a biometric information.

Our security improvement SI-NG-PON2 requires new PLOAM messages, as mentioned in Section 4. The specification of NG-PON2 networks defines several PLOAM messages but there is not full range specification. On the other words, a vendor is able to define own PLOAM message(s) between OLT and ONU. We rely on this fact with our solution, which may add overhead or delay in key establishment between OLT and ONU. OLT sends a request to ONU for key exchange phase, but OLT waits with a quite window interval. An ONU receives the request and answer with new PLOAM message and sends PLOAM message(s) in next BWmap allocation. Once the key is established, the ONU uses this key in bidirectional communication.

The direction of future work will be the implementation of the proposed security improvements in the real NG-PON2 network and a proposal of a solution for nonrepudiation of the data origin and delivery between ONUs in the NG-PON2.

Author Contributions: Conceptualization, V.C., T.H., and P.M. Methodology, V.C. and P.M. Validation, T.H. and V.O. Formal analysis, T.H. Investigation, V.C., T.H., P.M., V.O. Resources, T.H. and P.M. Writing, original draft preparation, V.C., T.H., P.M., and V.O. Writing, review and editing, V.C. and T.H. Visualization, V.O. Project administration, P.M. and T.H. Funding acquisition, P.M. and T.H.

Funding: The presented research has been supported by projects of the Ministry of the Interior of the Czech Republic under Grant No. VI20172019072 registration, E-infrastructure CESNET—modernization, registration number CZ.02.1.01/0.0/0.0/16_013/0001797; the National Sustainability Program under Grant No. LO1401; and partly by The Ministry of Education, Youth and Sports from the Large Infrastructures for Research, Experimental Development, and Innovations project reg. no LM2015070.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AES-CMAC	Advanced Encryption Standard cipher-based message authentication code
AES-CTR	Advanced Encryption Standard cipher operated in the counter mode
AES-ECB	Advanced Encryption Standard cipher with electronic codebook mode
C-IBS	Complementary index-based syndrome
CC	Correction code
CRPs	Challenge–response pairs
DRAM	Dynamic random access memory
EER	Equal error rate
FAR	False acceptance rate
FRR	False rejection rate

FSAN	Full Service Access Network
FTTH	Fiber to the home
GPON	Gigabit passive optical network
HD	Helper data
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet services provider
KEK	Key integrity key
LDPC	Low-density parity-check
MIC	Message integrity check
MRAM	Magnetoresistive random access memory
MRSPUF	Memristive device-based strong physical unclonable functions
MSK	Master session key
NG-PON2	Next-generation passive optical network stage 2
OCB	Offset codebook
ODN	Optical distribution network
OLT	Optical line termination
OLT CT	Optical line termination channel termination
OMCI	Optical network unit management and control interface
OMCI_IK	Optical network unit management and control interface integrity key
ONU	Optical network unit
P2P	Point-to-multipoint
PLOAM	Physical layer operations, administration, and maintenance
PLOAM_IK	Physical layer operations, administration, and maintenance integrity key
PON	Passive optical network
POWFs	Physical one-way functions
PUFs	Physical unclonable functions
RFID	Radio frequency identification
RM	Reed–Muller code
RS	Reed–Solomon code
SI-NG-PON2	Security improvement next-generation passive optical network stage 2
SK	Session key
TDM	Time division multiplex
TWDM	Time and wavelength division multiplex
XGEM	Next-generation passive optical network encapsulation method
XG(S)-PON	Next-generation (symmetric) passive optical network

References

1. Full Service Access Network. Available online: https://www.fsan.org/ (accessed on 5 May 2019).
2. Horvath, T.; Munster, P.; Vojtech, J. Deployment of PON in Europe and Deep Data Analysis of GPON. In *Telecommunication Systems [Working Title]*; InTech: London, UK, 2019; pp. 1–20.
3. Weissberger, A. Combined FTTH and DSL Spending Set to Slow until 10 Gbps PON and G.fast Deployments. Available online: http://techblog.comsoc.org/tag/market-forecast/ (accessed on 30 April 2019).
4. Hernandez, J.A.; Sanchez, R.; Martin, I.; Larrabeiti, D. Meeting the Traffic Requirements of Residential Users in the Next Decade with Current FTTH Standards: How Much? How Long? *IEEE Commun. Mag. (Early Access)* **2019**, *57*, 120–125. [CrossRef]
5. Ford, G.S. Is faster better? Quantifying the relationship between broadband speed and economic growth. *Telecommun. Policy* **2018**, *42*, 766–777. [CrossRef]
6. G.989.2: 40-Gigabit-Capable Passive Optical Networks 2 (NG-PON2): Physical Media Dependent (PMD) Layer Specification. Available online: https://www.itu.int/rec/T-REC-G.989.3 (accessed on 30 April 2019).
7. G.989.3: 40-Gigabit-Capable Passive Optical Networks (NG-PON2): Transmission Convergence Layer Specification. Available online: https://www.itu.int/rec/T-REC-G.989.3 (accessed on 8 April 2019).

8. *ISO/IEC 13888-2:2010—Information Technology—Security Techniques—Non-Repudiation—Part 2: Mechanisms Using Symmetric Techniques*, 2nd ed.; International Organization for Standardization: Geneva, Switzerland, 2010; p. 17.
9. Herder, C.; Yu, M.-D.; Koushanfar, F.; Devadas, S. Physical Unclonable Functions and Applications: A Tutorial. *Proc. IEEE* **2014**, *102*, 1126–1141. [CrossRef]
10. Pappu, R. Physical One-Way Functions. *Science* **2002**, *297*, 2026–2030. [CrossRef] [PubMed]
11. Mesaritakis, C.; Akriotou, M.; Kapsalis, A.; Grivas, E.; Chaintoutis, C.; Nikas, T.; Syvridis, D. Physical Unclonable Function based on a Multi-Mode Optical Waveguide. *Sci. Rep.* **2018**, *8*, 1–12. [CrossRef] [PubMed]
12. Grubel, B.C.; Bosworth, B.T.; Kossey, M.R.; Sun, H.; Cooper, A.B.; Foster, M.A.; Foster, A.C. Silicon photonic physical unclonable function. *Opt. Express* **2017**, *25*, 12710–12721, doi:10.1364/OE.25.012710. [CrossRef] [PubMed]
13. Anderson, B.R.; Gunawidjaja, R.; Eilers, H. Initial tamper tests of novel tamper-indicating optical physical unclonable functions. *Appl. Opt.* **2017**, *56*, 2863–2872. [CrossRef] [PubMed]
14. Das, J.; Scott, K.; Rajaram, S.; Burgett, D.; Bhanja, S. MRAM PUF: A Novel Geometry Based Magnetic PUF With Integrated CMOS. *IEEE Trans. Nanotechnol.* **2015**, *14*, 436–443. [CrossRef]
15. Tehranipoor, F.; Karimina, N.; Xiao, K.; Chandy, J. DRAM based Intrinsic Physical Unclonable Functions for System Level Security. In Proceedings of the 25th Edition on Great Lakes Symposium on VLSI—GLSVLSI '15, Pittsburgh, PA, USA, 20–22 May 2015; ACM Press: New York, NY, USA, 2015; pp. 15–20.
16. Tehranipoor, F.; Karimian, N.; Yan, W.; Chandy, J.A. DRAM-Based Intrinsic Physically Unclonable Functions for System-Level Security and Authentication. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2017**, *25*, 1085–1097. [CrossRef]
17. Gao, Y.; Ranasinghe, D.C.; Al-Sarawi, S.F.; Kavehei, O.; Abbott, D. Memristive crypto primitive for building highly secure physical unclonable functions. *Sci. Rep.* **2015**, *5*, 1–14. [CrossRef] [PubMed]
18. Dodis, Y.; Reyzin, L.; Smith, A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In *Advances in Cryptology—EUROCRYPT 2004*; Springer: Berlin, UK, 2004; pp. 523–540, doi:10.1007/978-3-540-24676-3_31. [CrossRef]
19. Dodis, Y.; Ostrovsky, R.; Reyzin, L.; Smith, A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.* **2008**, *38*, 97–139. [CrossRef]
20. Yu, M. -D.; Devadas, S. Secure and robust error correction for physical unclonable functions. *IEEE Des. Test Comput.* **2010**, *27*, 48–65. [CrossRef]
21. Hiller, M.; Merli, D.; Stumpf, F.; Sigl, G. Complementary IBS: Application specific error correction for PUFs. In Proceedings of the 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, San Francisco, CA, USA, 3–4 June 2012; pp. 1–6.
22. Muelich, S.; Puchinger, S.; Bossert, M.; Hiller, M.; Sigl, G. Error Correction for Physical Unclonable Functions Using Generalized Concatenated Codes. In Proceedings of the Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory ACCT2014, Svetlogorsk, Russia, 7–13 September 2014; pp. 1–6.
23. Puchinger, S.; Mueelich, S.; Bossert, M.; Hiller, M.; Sigl, G. On Error Correction for Physical Unclonable Functions. In Proceedings of the 10th International ITG Conference on Systems, Communications and Coding (SCC 2015), Hamburg, Germany, 2–5 February 2015; pp. 1–6.
24. Mueelich, S.; Bossert, M. A New Error Correction Scheme for Physical Unclonable Functions. In Proceedings of the 11th International ITG Conference on Systems, Communications and Coding (SCC 2017), Hamburg, Germany, 6–9 February 2017; pp. 1–6.
25. Horvath, T.; Malina, L.; Munster, P. On security in gigabit passive optical networks. In Proceedings of the 2015 International Workshop on Fiber Optics in Access Network (FOAN), Brno, Czech Republic, 6–7 October 2015; pp. 51–55.
26. Malina, L.; Munster, P.; Hajný, J.; Horvath, T. Towards Secure Gigabit Passive Optical Networks. In Proceedings of the12th International Conference on Security and Cryptography (SECRYPT 2015), Colmar, France, 20–22 July 2015; pp. 349–354.
27. Malina, L.; Horvath, T.; Munster, P.; Hajny, J. Security solution with signal propagation measurement for Gigabit Passive Optical Networks. *Optik* **2016**, *127*, 6715–6725. [CrossRef]
28. Song, J.H.; Poovendran, R.; Lee, J.; Iwata, T. RFC4493—The AES-CMAC Algorithm. Available online: https://tools.ietf.org/html/rfc4493 (accessed on 8 April 2019).

29. Lipmaa, H.; Wagner, D.; Rogaway, P. Comments to NIST Concerning AES Modes of Operation: CTR-Mode Encryption. Available online: https://bit.ly/2OTohab (accessed on 8 April 2019).
30. Daemen, J.; Rijmen, V. *The Design of Rijndael: AES—The Advanced Encryption Standard*; Springer: Berlin, Germany, 2002; p. 238.
31. Apostol, K. *Brute-Force Attack*; SaluPress: USA, 2012.
32. Suh, G.E.; Devadas, S. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In Proceedings of the 2007 44th ACM/IEEE Design Automation Conference, San Diego, CA, USA, 4–8 June 2007; pp. 9–14.
33. Maes, R. *Physically Unclonable Functions: Constructions, Properties and Applications*; Springer: New York, NY, USA, 2013; p. 172.
34. Bohm, C.; Hofer, M. *Physical Unclonable Functions in Theory and Practice*; Springer: New York, NY, USA, 2013; p. 263.
35. Maes, R.; Verbauwhede, I. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. In *Towards Hardware-Intrinsic Security*; Springer: Berlin, Germany, 2010; pp. 3–37._1. [CrossRef]
36. Horvath, T.; Clupek, V.; Munster, P.; Oujezsky, V. Key Exchange with PUF in NG-PON2 Networks. In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 118–121.
37. Dworkin, M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. Available online: https://bit.ly/2XWVuVo (accessed on 1 May 2019).
38. Dworkin, M. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. Available online: https://csrc.nist.gov/publications/detail/sp/800-38c/final (accessed on 1 May 2019).
39. Bellare, M.; Rogaway, P.; Wagner, D. The EAX Mode of Operation. In *Fast Software Encryption*; Lecture Notes in Computer Science; Springer: Berlin, Germany, 2004; pp. 389–407.
40. Stallings, W. The offset codebook (OCB) block cipher mode of operation for authenticated encryption. *Cryptologia* **2018**, *42*, 135–145 doi:10.1080/01611194.2017.1422048.
41. Dworkin, M. NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf (accessed on 10 April 2019).
42. Xi, X.; Zhuang, H.; Sun, N.; Orshansky, M. Strong subthreshold current array PUF with 2^{65} challenge–response pairs resilient to machine learning attacks in 130nm CMOS. In Proceedings of the 2017 Symposium on VLSI Circuits, Kyoto, Japan, 5–8 June 2017; pp. C268–C269.