Physically Related Functions: A New Paradigm for Light-weight Key-Exchange

Durba Chatterjee¹, Harishma Boyapally¹, Sikhar Patranabis², Urbi Chatterjee³, Deepend Mukhopadhyay¹, Aritra Hazra¹
1. Indian Institute of Technology Kharagpur, 2. ETH Zurich, 3. Indian Institute of Technology Kanpur

ABSTRACT
In this paper, we propose a novel primitive named Physically Related Function (PReF) which are devices with hardware roots of trust. It enables secure key-exchange with no pre-established/embedded secret keys. This work is motivated by the need to perform key-exchange between lightweight resource-constrained devices. We present a proof-of-concept realization of our contributions in hardware using FPGAs.

Keywords: Boolean functions, Key-exchange protocol, Physically Related Functions

1 INTRODUCTION
The most straightforward way of achieving secure key-exchange is via standard cryptographic techniques, where an initially exchanged secret key allows the devices to encrypt all ensuing communication. However, these devices are far too resource-constrained to either support the heavy protection mechanisms against invasive and semi-invasive attacks [8] associated with secure key-storage (as in symmetric-key primitives) or does not have provisions for renewal of certificates (as in asymmetric-key primitives). This is a scenario frequently encountered today with the widespread advent of Internet of Things (IoT) and Cyber-Physical Systems (CPS). Amazon, Uber, and UPS and other major corporations have recently announced plans to launch commercial autonomous drone operations [3, 4]. The widespread deployment of such technologies would potentially involve millions of devices communicating with each other. This makes it essential to design light-weight protocols for secure communication that can scale to a large number of devices.

In this paper, we introduce novel hardware primitives called Physically Related Functions (abbrv. PReFs). We present a PReF-based on-the-fly key-exchange scheme, without the need to store any secret key or the need to contact any trusted third party. We present a proof-of-concept (PoC) realization of PReFs in hardware using 94 separate Xilinx Artix 7 FPGAs.

2 PHYSICALLY RELATED FUNCTIONS
A pair of PReFs (DA, DB) physically implement the functions (fA, fB) with input space X and output space Y such that there exists a specific subset of inputs XAB ⊆ X such that the output behaviors of the functions fA and fB on each input in XAB are correlated with respect to some distance metric (eg. Hamming Distance (HD)). On the other hand, for any x ∈ X \ XAB, any probabilistic poly-time bounded algorithm that only has access to an implementation of fA and does not not have (even black-box) access to an implementation of fB cannot distinguish fB(x) from random. This is defined as the pseudorandomness property of PReFs.

Figure 1: Basic Key Exchange

PReF-based Key Exchange Scheme
Now, we develop a key-exchange scheme for secure communication between two devices in a PReF network. Our protocols preclude the usage of long-term secure key storage, as is usually the case with a large class of key-exchange protocols based on traditional cryptographic approaches [1, 6]. In other words, it avoids not only the need for dedicated key storage but also the associated countermeasures for preventing potential physical attacks (both invasive and non-invasive) targeting such key storage. It is also superior to the key-exchange schemes based on alternative primitives (such as Physically Uncloneable Functions (PUFs)) which are asymmetric in nature requiring one (or both) device(s) to perform complex computations or require trusted third party during the protocol run. So, in a way, our scheme achieves the best of both worlds, especially in the context of lightweight resource-constrained devices.

Protocol Description. Let (DA, DB) be a pair of PReFs as described previously, such that X = {0, 1}m and Y = {0, 1}n. These devices form a PReF pair over the input subset XAB ⊆ X such that for any x ∈ XAB, HD(fA(x), fB(x)) ≤ δ. Let (E, D) be the encoding and decoding algorithms of an (n, k, δ) linear error correction code (ECC).

We present a basic PReF-based key exchange protocol as described in Fig. 1, that requires no computational resources beyond evaluating PReF outputs. It enables a key exchange between two PReF devices DA and DB with the unique "related" input set XAB. The protocol involves a single round of communication between the devices and is considerably light-weight given that it only uses error-correcting codes in addition to PReFs.

Theoretical Implications. This protocol also has some interesting theoretical implications about the computational power of PReFs. It is well-known that no computationally secure key-exchange protocol (even multi-round) can be based in a black-box manner on purely symmetric-key cryptographic primitives such as pseudorandom functions or symmetric-key encryption [5]. The fact that we can bypass this impossibility result using only PReFs and no additional cryptographic primitives/trusted parties indicates that PReFs are, in fact, more powerful than simple symmetric-key cryptographic primitives. This makes PReFs an interesting object of study from a cryptographic standpoint.
which X
where X
and let 𝑥
and 𝜖
occurs, for any
subset
For a more generic analysis, consider the functions
statistically uncorrelated, there exist some inputs for which both
C
from the space of all
X
for two Boolean functions
inputs for any pair of random Boolean functions.

Overview of output-correlation estimation between two
devices embodying a pair of ReFs.

In this section, we establish the feasibility of embedding “related”
functions into physical devices, i.e., the feasibility of realizing PReFs
in hardware. We show that the notion of correlation with respect
to Hamming distance (HD) allows us to obtain a set of “related”
inputs for any pair of random Boolean functions.

Correlation Analysis of Boolean Functions. In Boolean theory,
the cross-correlation function [7] is used to study the cryptographic
properties of Boolean functions. The cross-correlation function
for two Boolean functions 𝑓 : 𝑋 → 𝑌 and 𝑔 : 𝑋 → 𝑌 where
𝑋 = \{0, 1\}ⁿ and 𝑌 = \{0, 1\} calculates the correlation between its
outputs over the complete input set 𝑋. It is given by:

\[ C_{𝑓,𝑔} = \frac{1}{|𝑋|} \sum_{𝑥∈𝑋} (-1)^{𝑓(𝑥)⊕𝑔(𝑥)} \]

and its value lies in [−1, 1]. Now, if the functions 𝑓 and 𝒔 are chosen
uniformly at random from the space of all 𝑛-bit Boolean functions,
their outputs will be statistically uncorrelated. Hence, 𝐶_{𝑓,𝑔} = 0.

For this work, we have exploited the fact that even if 𝑓 and 𝒔
are statistically uncorrelated, there exist some inputs for which both
have the same outputs. We can split 𝑋 into two disjoint subsets 𝑋₀
and 𝑋₁ such that 𝑓(𝑥) = 𝑔(𝑥) ∀𝑥 ∈ 𝑋₀ and 𝑓(𝑥) ≠ 𝑔(𝑥) ∀𝑥 ∈ 𝑋₁.
Therefore, we can say that 𝑓 and 𝒔 are related over the subset 𝑋₀.
For a more generic analysis, consider the functions 𝑓ₓ₀, 𝑓ₓ₁ : 𝑋 → 𝑌,
where 𝑋 = \{0, 1\}ⁿ and 𝑌 = \{0, 1\}ᵐ. To find the input subset over
which 𝑓ₓ₀ and 𝑓ₓ₁ are split, we split the input set into disjoint subsets
\{0₀, 0₁, ⋯, 0ₘ\}, such that for any input belonging to subset
0ᵢ, the HD between the function outputs is 𝑖. Note that the HD
is calculated over the 𝑚-bit response.

Let \( f_{x}(i)[i] \) denote the 𝑖ᵗʰ bit of the output of \( f_{x} \) for an input
\( x \) and let \( q \) be the probability with which \( f_{x}(i)\{i\} \) \& \( f_{y}(i)\{i\} \) = 1
occurs, for any \( i \in [1, m] \). The probability that HD(\( f_{x}(i)\), \( f_{y}(i)\))
takes the value \( j \in [0, m] \) can be given as:

\[ \Pr[\text{HD}(f_{x}(i), f_{y}(i)) = j] = \binom{m}{j} q^j (1 - q)^{m-j}. \]  \( (1) \)

From the above equation, it is evident that the frequency
distribution calculated using the HD follows a Binomial distribution.
Let \( ε_{AB} \) denote the probability with which HD(\( f_{x}(i)\), \( f_{y}(i)\)) ≤ \( δ \)
holds. We can calculate \( ε_{AB} \) as:

\[ ε_{AB} = \Pr[\text{HD}(f_{x}(i), f_{y}(i)) \leq δ] = \sum_{j=0}^{δ} \binom{m}{j} q^j (1 - q)^{m-j}. \]  \( (2) \)

Then the size of the input subset \( X_{AB} \subseteq 𝑋 \), over which the outputs
of \( f_{x} \) and \( f_{y} \) have HD almost \( δ \) is given as:

\[ |X_{AB}| = ε_{AB} |X|. \]  \( (3) \)

A pair of functions \( f_{x} \) and \( f_{y} \) are said to be related if \( X_{AB} \neq \emptyset \)
and \( ε_{AB} > 0 \). Thus with this notion of output-correlation, we can
obtain “related” inputs for any pair of random Boolean functions.

As already mentioned, our aim is to realize PReFs using hardware
devices. Equipped with this analysis, we simply design Boolean
functions as hardware circuits and rely on the internal variability of
every device to introduce unpredictable yet repetitive randomness
in the circuit behaviour.

4 EXPERIMENTAL EVALUATION

We present a proof-of-concept (PoC) realization of PReFs, using
PUFs for embedding Boolean functions in hardware devices and
a prototype evaluation of the PReF-based KE protocol. For the
PoC realization of the PReF constructs, we deploy the PUF design
proposed in [2] in 84 Artix-7 FPGAs which takes 64-bit binary
input and generates 224-bit binary output. To identify the “related”
input subsets, we characterise every PUF with 20K random inputs
and calculate HD of the outputs for every pair. We observe that
HD follows Binomial distribution which corroborates with our
theoretical analysis presented in Sec. 3. We filter the challenges
for which the HD is less than a pre-determined threshold \( δ \) (ref.
Fig. 2). Next, we find the true positive rate (TPR) and false positive
rate (FPR) of protocol. To calculate TPR, we randomly choose 1000
inputs over which a pair of related devices can communicate. We
observe that the probability that two devices establish the same
key is 100%, for all the 1000 inputs. We use the same inputs to find
the probability (FPR) that an illegitimate device (not related over
the chosen input subset) can successfully exchange the key with
a legitimate device. The FPR of the protocol is observed to range from 2⁻⁹⁰ to 2⁻¹⁰ for all the 1000 inputs.

5 CONCLUSION AND FUTURE WORK

In this paper, we initiated the study of Cryptophasia in Hardware
using a novel class of hardware primitives called Physically Related
Functions (PReFs) that have not been studied before to the best of our
knowledge. We demonstrated how PReFs can be used to establish
a key-exchange scheme with no pre-established secure channels
and no secure storage for cryptographic keys. We established the
feasibility of our proposal via concrete prototype implementations
and extensive experimental implementations on Artix-7 FPGAs.

As a future work, we will build authenticated key-exchange schemes
for a network of resource-constrained devices, ensuring secure
communication between any two devices.

REFERENCES