Re-implementation of the Picnic signaturescheme in Python

Thorsten Knoll

info@thorstenknoll.de

March, 2019

I. Introduction

Post-quantum cryptography, NIST and Picnic

Quantum computers are experiencing fast development and seem to be available within a timeframe of the next few decades. One of their properties will be to break huge parts of modern cryptography. Especially the discrete logarithm and prime-factorisation loose their trapdoor funcionality in regards to the efficient quantum algorithms from Grover and Shor. Therefore the need for new cryptographic algorithms arises, beeing save in regards to the availability of quantum computers. This field of research goes with the name "Post-quantum cryptography" (PQC). The american National Institute of Standards and Technology (NIST) called out a challenge to find the next PQC standards. This challenge is in round two of three at the time of writing this document. 69 submissions from round one were reduced to 26 candidates in round two of the challenge. These 26 candidates got announced by NIST not long ago at the end of january 2019. One of the submissions surviving the first round is the Picnic signaturescheme.

NIST PQC page: `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`

Evaluation and reviews

69 submissions is quite a huge amount in terms of reviewing and evaluating them. Additionaly PQC is a new field of research with a history not much longer than a decade. Cryptographers (and -analysts) are working intense on creating, evaluating, reviewing and breaking PQC algorithms. The state of PQC is that every litte step helps towards the goal of having secure PCQ algorithms. At RheinMain University of Applied Sciences (HSRM) the Master Students in Computer Science found together in a research course to participate in this process. This re-implementation is part of this efford.

Goals: Learning Picnic (and LowMC)

The sole purpose of this re-implementation is learning and understanding the Picnic algorithm and it's underlying zero-knowledge proof system. The goals are to provide an "easy to read and understand" codebase in a high-level language (Python) and make it a little easier to follow and learn the designprinciples of Picnic. The execution of Python-Picnic is awefull slow compared to the reference implementations in C. It is very unlikely that this will ever reach a usable state for production. Additionaly the code is not reviewed by anyone but the author and is surely not secure for productive use. But it may help to understand Picnic.

On the way to understand Picnic, another algorithm must be understood too. That is the LowMC blockcipher. There are two main parts in Picnic, where LowMC plays a major role. Firstly the derivation of the public key is a LowMC encryption of the Picnic private key. Secondly each Picnic zero-knowledge round is a modified LowMC encryption, fitted into a Multi-Party-Computation (MPC) scheme. In the following description of the implementations we start with LowMC for that reason.

Reference documents and implementations by the Picnic Team

The original publications and reference implementations (in C) are available at:

Microsoft Picnic projectpage: `https://www.microsoft.com/en-us/research/project/picnic/`
Microsoft Picnic Github: `https://github.com/Microsoft/Picnic`

Re-implementations in Python

These re-implementations in Python follow the original MIT Licenses and are public available at:

LowMC in Python: `https://github.com/ThorKn/Python-LowMC`
Picnic in Python: `https://github.com/ThorKn/Python-Picnic`

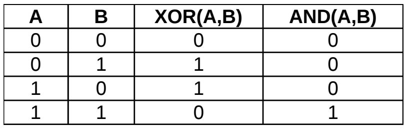
Installation and usage instructions are given inside the projects `README` files. This `PDF` can be found inside the `Python-Picnic` project in the `docs` folder.

II. LowMC

Idea and overview

Picnic makes intense use of the LowMC algorithm. Therefore we start with LowMC before hopping over to Picnic. A standalone LowMC Python-implementation got build as a starting point to understand Picnic. That is why there is a own Github project under the name `"Python-LowMC"`.

LowMC is a blockcipher in a roundbased construction scheme like many other blockciphers. The name is an abbreviation for "Low multiplicative complexity". XOR in GF2 is a linear operation (ADD), while the multiplication (AND) in GF2 is a non-linear operation (Figure 1). LowMC tries to keep the count of AND operations as low as possible while still maintaining a given security level (L1, L3, L5). Additionaly LowMC is also designed to keep the AND-depth low. That means most AND operations could be done in parallel.



A	B	XOR(A,B)	AND(A,B)
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Figure 1: Linear and non-linear operations

Figure 2 shows the roundbased scheme of LowMC. Only the sbox part of the algorithm uses multiplications (ANDs). The other parts strictly contain only linear operations. From a mathematical point of view the XOR is a bijective function and the multiplications (ANDs) in GF2 are not bijective. Therefore the sboxes are the only not bijective part in LowMC. That is the reason for choosing LowMC in Picnic and it keeps the signature lengths smaller than with other blockciphers. We'll see how this is achieved with the Picnic implementation later on.

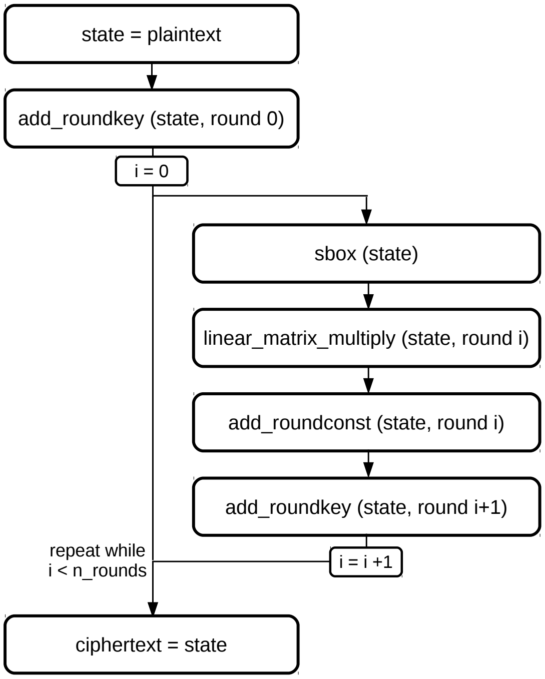

state = plaintext
add_roundkey (state, round 0)
i = 0
sbox (state)
linear_matrix_multiply (state, round i)
add_roundconst (state, round i)
add_roundkey (state, round i+1)
repeat while
i < n_rounds
i = i +1
ciphertext = state

Figure 2: LowMC scheme

Pre-calculated constants

The python program `generator.py` generates the files for all security levels with the following pre-calculated constants:

- Linear layer matrices
- Round constants
- Roundkey matrices

The generation of the constants-files is not mandatory for usage as the project contains them "ready to use".

Private functions

`__apply_sbox()`

Sboxes are the only parts in LowMC, that contain multiplications in GF2 (ANDs). A fixed number of sboxes is applied to the state. Each sbox substitutes 3 Bit of the original state through a fixed substitution scheme. Let a, b and c be three bits in the state. Then a', b' and c' get computed by:

$$a' = a \oplus b \cdot c$$
$$b' = a \oplus b \oplus a \cdot c$$
$$c' = a \oplus b \oplus c \oplus a \cdot b$$

Where $\oplus$ is XOR and $\cdot$ is AND. So each 3-Bit sbox contains exactly 3 multiplications (ANDs). The security level (L1, L3, L5) defines the number of 3-Bit sboxes (n) per LowMC-round as shown in figure 3. The surplus Bits in the state get no substitution, shown on the right of the figure. The total number of multiplications for a complete encryption in LowMC sums up to $3 * n * rounds$. In example for security level L1 this calculates to $3 * 10 * 20 = 600$ ANDs.

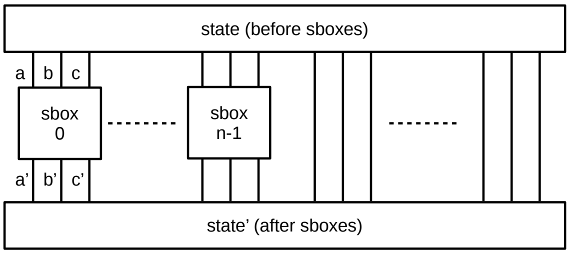


Figure 3: Sboxes per LowMC round

The function applies the sboxes to a state in memory and has no parameters and no returns. The actual state is stored in the private variable `self.__state`. The sboxes are stored as a list (you can imagine it as a lookup-table) in the private variable `self.__sbox`.

`__multiply_with_lin_mat(round)`

The state gets matrix multiplied with the constant and pre-calculated linear matrix. This contains only linear operations.

`Add roundconstant`

This needs no seperate function. It is a one-line operation with XOR on the state and therefore contains only linear operations.

`__key_addition(round)`

For XOR'ing the roundkey to the state the roundkey must be derived first. This is done by a matrix multiplication of the private key and the constant, pre-calculated roundkey-matrix. Again this only contains linear operations.

`Decryption functions`

The decryption works pretty much the whole encryption way backwards. For the matrix multiplications their inverse matrices are needed. They get calculated within the constructor of the LowMC class and stored in seperate, private variables. The neccessary functions are named like the ones for encryption but with a `_inv` appended to their names. The same rule applies for the names of their private variables.

Public functions (API)

`LowMC(Security level) - Constructor`

Constrcuts an object of LowMC with the parameters regarding to the security level. The following security levels are available and shall be given to the constructor as strings: "picnic-L1", "picnic-L3" and "picnic-L5". The fitting file with the constants must be in the project directory and gets read (see Pre-calculated constants). The constants from the file get stored in the private variables `self.__lin_layer`, `self.__round_consts` and `self.__round_key_mats`.

`generate_priv_key()`

Generates a private key of the length specified within the security level. The private key is stored in the private variable `self.__priv_key`. The CSPRNG from the python package `os` is used (`os.urandom(bytelength)`).

`set_priv_key(priv_key)`

Instead of generating the private key, it can also be set by giving a bytearry to this function. The bytearray must match the specified keylength from the security level.

`encrypt(plaintext)`

Encrypts a plaintext and returns the ciphertext. The plaintext length must match the specified blocksize length (security level) and must be given as a bytearray to the function. The ciphertext is returned as a bytearray of the same length. Before using this function a private key must be set (or generated).

`decrypt(ciphertext)`

Decrypts a ciphtertext and returns the plaintext. The ciphertext length must match the specified blocksize length (security level) and must be given as a bytearray to the function. The plaintext is returned as a bytearray of the same length. Before using this function a private key must be set (or generated).

Testvectors

The repository contains the python file `test_lowmc.py`. One can simply run this and nine different testvectors get executed on the implementation. Three vectors for each security level. This testfile is also a good starting point to see how the implementation can be used.

Prerequisites

The code is tested with Ubuntu 16.04 LTS and Python3.6. The package "BitVector" for python is required. It is recommended to use a virtual environment for Python, like `virtualenv`. In (very) short lines:

```
virtualenv -p /usr/bin/python3.6 myvenv
source /path_to_myvenv/bin/activate
<myvenv>pip install BitVector
<myvenv>python test_lowmc.py
```

III. Picnic

Components

Picnic is a Post-quantum signature scheme that does not rely on hard number theoretical problems like discrete logarithm or prime-factorization. Instead Picnice embedds symmetric cryptographic primitves into a zero-knowledge proof system. The components of Picnic are:

- A blockcipher (LowMC)
- A Hashfunktion (SHA3-SHAKE)
- A Zero-knowledge proof system (ZKB++)

LowMC is discussed earlier in this document. It is a parametric blockcipher algorithm that simulates a gatebased (XOR, AND in GF2) electrical circuit from input to output with low AND-gate counts. The Python-LowMC implementation will be used for Picnic. SHA3-SHAKE will not be discussed in detail in this document. It is a NIST-standardized Hashalgorithm, based on the Spongeconstruction with an arbitrary output length. In Picnic SHA3-SHAKE is used as a Hashfunction as well as a Key-Derivation-Function (KDF). Python-Picnic uses the Python library `hashlib` whereever SHA3-SHAKE is needed

That leaves the zero-knowledge proof system ZKB++ to explain. The following descriptions are on a very abstract level and will not explain every detail. Instead we'll focus on getting a broad overview of the functionality to learn the key points of the implementation. Most of the following examples are based on the documentations and presentations of the Picnic research team [1].

Proof of knowledge: The Σ - Protocol

Zero-knowledge proofs are based on the Σ-protocol, but with the twist to transmitt no parts of the underlying secret anywhere in the communication. The basic Σ-Protocol is a communication scheme between two parties as in figure 4. A prover wants to convince a verifier about the knowledge of a secret.

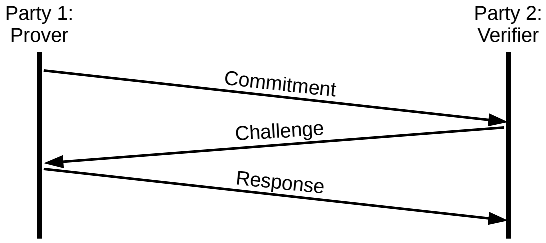


Figure 4: Σ-Protocol scheme

To prove this knowledge, a 3-way communication is held. A classic example for the Σ-Protocol is the Schnorr protocol. It is based on the discrete logarithm. The prover knows a secret x so that $y = g^x$ with g beeing a generator in a cyclic group G_p with the order p. The messages in the Schnorr protocol are:

[1] https://asiacrypt.iacr.org/2018/files/SLIDES/TUESDAY/Z411/post%20quantum%20signatures%20-%20asiacrypt18v2.pdf

- Commitment: Prover chooses a random r and commits $t = g^r$ and y.
- Challenge: Verifier chooses a random c and sends it to the prover.
- Response: Prover sends $s = r + cx$.

The verifier accepts, if $ty^c = g^s$. Because:

$$ty^c = g^r y^c = g^r g^{cx} = g^{r+cx} = g^s$$

Inserted into the sequence diagramm above, this communication would look like figure 5.

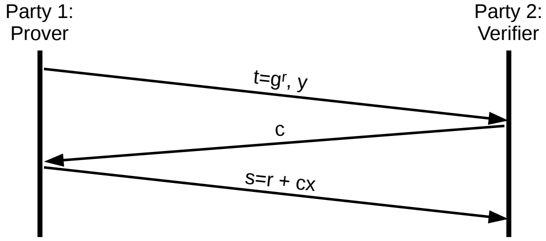


Figure 5: Schnorr protocol

LowMC in ZKB++

In the next step towards ZKB++ we'll look into how LowMC works as the One-way-function inside a Σ-protocol.

Imagine LowMC as a electronic circuit of XOR and AND gates as in the example in figure 6. There are inputs ($x_{1..8}$) and outputs ($y_{1..6}$) from the circuit. The function of this LowMC circuit could be $f_{LowMC}(x) = y$. For given inputs the outputs can be calculated efficiently. For given outputs there is no efficient algorithm to determine the inputs. That is a hard to reverse function.

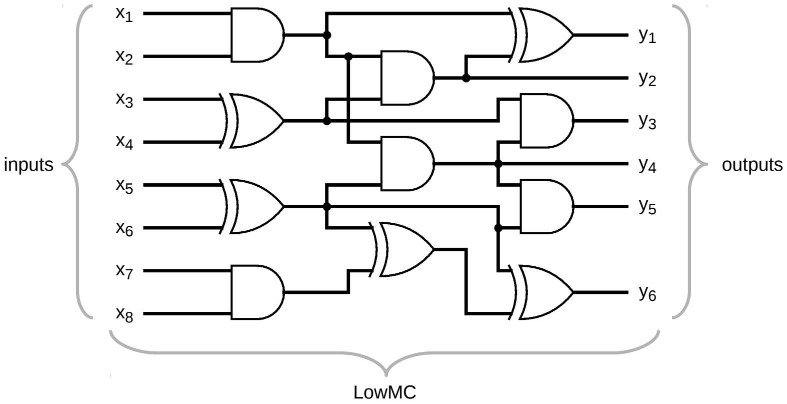


Figure 6: A LowMC circuit as a One-way-function

Thinking in terms of the Σ-protocol we can define the following sentence:

> *A prover has knowledge of a secret key (inputs x) that computes with the LowMC cicruit (One-way-function) to a public key (outputs y).*

MPC and the zero-knowledge proof

The zero-knowledge proof system ZKB++ is based on Multi-Party-Computation (MPC). MPC means that the prover from the Σ-protocol is splitted into different players. For ZKB++ the number of players is fixed to three. To get a grip of how MPC and the zero-knowledge property works, we'll look into an example from Melissa Chase from the Picnic research team (figure 7. She presented this example at RealWorldCrypto 2018 and the talk is public available as a video[2].

A prover knows the secrets a and b. The function f shall be the very simple circuit $c = a \oplus c$, where $\oplus$ is an XOR. Let H be a cryptographic secure Hashfunction (i.e. SHA3-SHAKE). This example is designed for two players, instead of the three players in ZKB++.

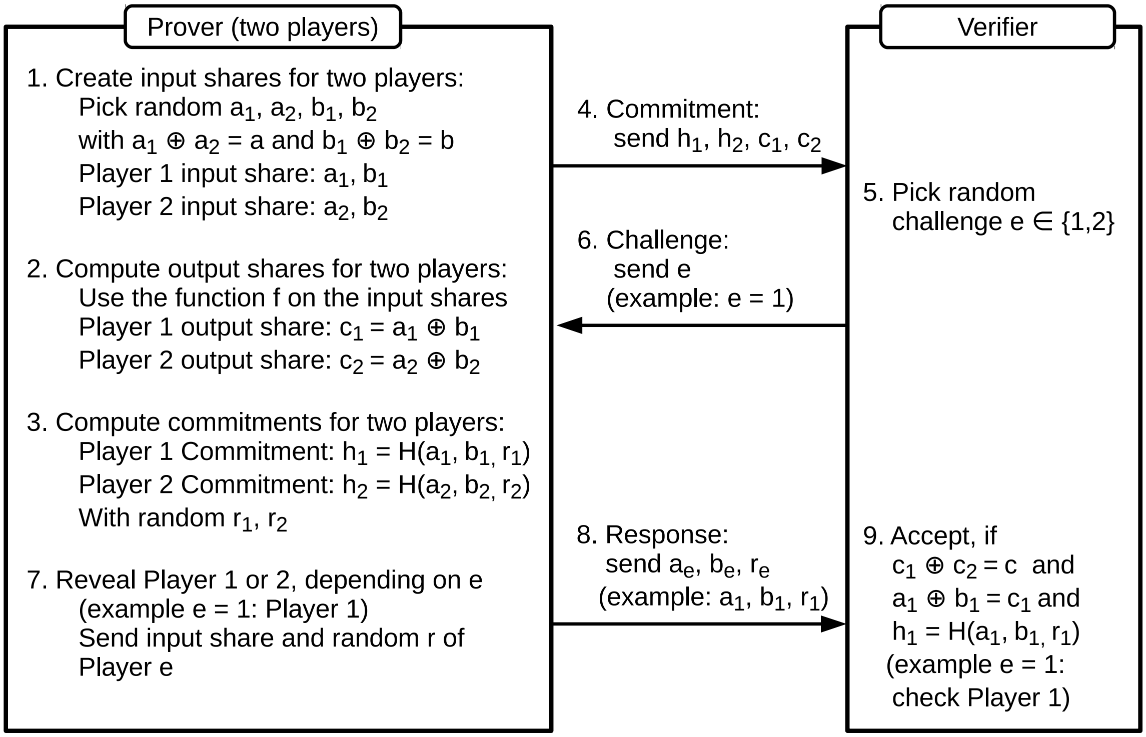

Prover (two players)
1. Create input shares for two players:
Pick random a_1, a_2, b_1, b_2
with $a_1 \oplus a_2 = a$ and $b_1 \oplus b_2 = b$
Player 1 input share: a_1, b_1
Player 2 input share: a_2, b_2
2. Compute output shares for two players:
Use the function f on the input shares
Player 1 output share: $c_1 = a_1 \oplus b_1$
Player 2 output share: $c_2 = a_2 \oplus b_2$
3. Compute commitments for two players:
Player 1 Commitment: $h_1 = H(a_1, b_1, r_1)$
Player 2 Commitment: $h_2 = H(a_2, b_2, r_2)$
With random r_1, r_2
7. Reveal Player 1 or 2, depending on e
(example e = 1: Player 1)
Send input share and random r of Player e
4. Commitment:
send h_1, h_2, c_1, c_2
6. Challenge:
send e
(example: e = 1)
8. Response:
send a_e, b_e, r_e
(example: a_1, b_1, r_1)
Verifier
5. Pick random challenge $e \in \{1,2\}$
9. Accept, if
$c_1 \oplus c_2 = c$ and
$a_1 \oplus b_1 = c_1$ and
$h_1 = H(a_1, b_1, r_1)$
(example e = 1: check Player 1)

Figure 7: MPC with two players

It is easy to recognize the Σ-protcol in this MPC by the message scheme of "commitment", "challenge" and "response". The differences are that now two players are involved on the prover side. Both have their input- and output shares and the challenge determines which players input shares get revealed. The verifier can then check if the revealed player had a valid input share of the secrets a and b and therefore is convinced about the provers knowledge of the secrets by a probability of 50% (one of two players). This can be repeated n times till the wanted probability (defined by the security level) is reached. The probability calculates to $p = (1/2)^n$. As the function f is assumed to be "hard to reverse", nothing about the secrets a and b got learned. That is the zero-knowledge part of the proof.

[2] `https://www.youtube.com/watch?v=_J9ESIy8D2o`

Some remarks about the differences between this example and the MPC in Picnic need to be noted:

- This works because of $(a_1 \oplus a_2) \oplus (b_1 \oplus b_2) = (a_1 \oplus b_1) \oplus (a_2 \oplus b_2) = c_1 \oplus c_2 = c$
- LowMC has AND gates. This makes dividing the shares more complicated.
- ZKB++ has three players instead of two. The secrets have to be shared by three.
- The cheating probability increases to 2/3. Confidence probability is $p = (1/3)^n$.
- Challenges request two players to be revealed with $e \in \{0, 1, 2\}$.
- The lowest security level in Picnic has $n = 219$ MPC rounds.

MPC in the head and Random oracle models

The zero-knowledge proof we've discussed so far is interactive. The verifier picks random challenges and sends them to the prover. It is wanted to calculate the proof without the need for an "external" source of randomness. This is called "MPC in the head" and reduces the proof to a non-interactive version. It wouldn't be a secure idea to let the prover choose the challenges on his own. The prover then could simply pick the challenge that favours him. A proveable solution to this is to use a "Random Oracle Model" (ROM) on the provers side to generate the challenges. In ZKB++ this is done with the cryptographic secure hashfunction SHA3-SHAKE. The commitments from each MPC round gets hashed and the challenges are extracted from this hash bitwise. In the example above (figure 7) this would be the hash of h_1, h_2, c_1, c_2.

Picnic has two different versions of MPC in the head implemented. The first one is the Fiat-Shamir (FS) transformation, which is based on the described ROM but might not be quantum save. The second option is the Unruh (UR) transformation, which is based on a Quantum Random Oracle Model (QROM). The re-implementation Python-Picnic can only handle the FS transformation so far.

The Picnic loops

Keys, Message and Signature

References

[1] Microsoft *Picnic PQC Signatureschene.* 2018