ETH Zurich, Department of Computer Science — Dr. Jonathan Bootle
HS 2023 — Karen Klein, Varun Maram, Antonio Merino Gallardo

Zero-Knowledge Proofs
Exercise 9 (graded)

Submission Deadline: 24/11/2022, 23:59 CEST

Note: Solutions must be typeset in LaTeX. Make sure to name the pdf file of your solutions in the following format:

"*<Legi Number>_9.pdf*"

9.1 An Interactive Protocol for Block Cipher Evaluation (20 marks)

In this exercise, you will use a variant of the GKR protocol to prove that a round of a block cipher loosely based on AES was computed correctly.[1]

Let $\mathbb{F}$ be a finite field. Let $K \in \mathbb{F}$ be a key. Consider the following construction of a single round $C\colon \mathbb{F}^{N^2} \to \mathbb{F}^{N^2}$ of a block cipher, represented by a layered circuit with depth $D = 3$ and layer size $S = N^2$, where $N = 2^n$.

- The input to C at the input layer 3 is a *state* in $\mathbb{F}^{N^2}$, which can be viewed as a matrix

$$W_3 = \begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,N-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{N-1,0} & x_{N-1,1} & \cdots & x_{N-1,N-1} \end{pmatrix} \in \mathbb{F}^{N\times N} \ .$$

- At layer 2, the state W_2 is obtained from W_3 by applying the function $x \mapsto (x+K)^3$ to every field element in the state.
- At layer 1, the state W_1 is obtained from W_2 by moving $x_{i,j}$ from position (i,j) to position $\mathsf{ShiftRows}(i,j) := (i, j-i \bmod N)$ i.e.

$$\begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,N-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{N-1,0} & x_{N-1,1} & \cdots & x_{N-1,N-1} \end{pmatrix} \mapsto \begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,N-1} \\ x_{1,1} & x_{1,2} & \cdots & x_{1,0} \\ \vdots & \vdots & \ddots & \vdots \\ x_{N-1,N-1} & x_{N-1,0} & \cdots & x_{N-1,N-2} \end{pmatrix} .$$

- At layer 0, the output state W_0 is obtained from W_1 using the mapping $W_0 = M \cdot W_1$, where $M \in \mathbb{F}^{N\times N}$.

a) Let $G_1(X_1,\ldots,X_m),\ldots,G_L(X_1,\ldots,X_m)$ be polynomials of total degree d over $\mathbb{F}$ representing *custom gates* mapping $\mathbb{F}^m \to \mathbb{F}$. Consider a layered circuit in which the k-th layer contains *only* gates $G_1,\ldots,G_L$ whose locations are described by functions $\mathsf{Custom}_1,\ldots,\mathsf{Custom}_L\colon \{0,1\}^{\ell_k} \times \left(\{0,1\}^{\ell_{k+1}}\right)^m \to \{0,1\}$.

Using $G_1,\ldots,G_L$ and $\mathsf{Custom}_1,\ldots,\mathsf{Custom}_L$, write down a summation equation connecting the values of the wire functions at level k and level $k+1$. [1 mark]

When $m \geq 2$, explain in detail how to modify the sumcheck and 2-to-1 reductions in the GKR protocol to verify the correct evaluation of the circuit. State the soundness

[1] We make no claims about the security of this block cipher!

errors and communication costs of the modified reductions in terms of m, d, ℓ_k, ℓ_{k+1}, and $|\mathbb{F}|$. [4 marks]

b) Write down a single custom gate $G\colon \mathbb{F} \to \mathbb{F}$ for layer 2 of C, and a function Custom describing the locations of G. [1 marks]

c) View W_k, W_{k+1} as functions $\{0,1\}^{2n} \to \mathbb{F}$, and $\mathsf{ShiftRows}$ as a function $\{0,1\}^{2n} \to \{0,1\}^{2n}$. Show that the following two statements are equivalent:

$$\forall \mathbf{i} \in \{0,1\}^{2n}, \quad W_k(\mathbf{i}) = W_{k+1}(\mathsf{ShiftRows}^{-1}(\mathbf{i})) \ , \tag{1}$$

$$\forall \mathbf{i} \in \{0,1\}^{2n}, \quad W_k(\mathbf{i}) = \sum_{\mathbf{j} \in \{0,1\}^{2n}} \mathsf{Eq}(\mathbf{i}; \mathsf{ShiftRows}(\mathbf{j})) \cdot W_{k+1}(\mathbf{j}) \ . \tag{2}$$

[2 marks]

d) Given functions $W_k, W_{k+1}\colon \{0,1\}^{2n} \to \mathbb{F}$ satisfying Equation (1), give an interactive protocol reducing a claim of the form "$\widetilde{W}_k(r_1, \ldots, r_{2n}) = v_k$" to a claim of the form "$\widetilde{W}_{k+1}(s_1, \ldots, s_{2n}) = v_{k+1}$". Prove that your protocol is complete and sound, clearly stating its soundness error. [7 marks]

e) Given matrices W_0, M and $W_1 \in \mathbb{F}^{N \times N}$ such that $W_0 = M \cdot W_1$, write down an explicit expression for the (i,j)-th entry of W_0 in terms of the entries of M and W_1. Hence, describe a method for reducing claims about the MLE of the output state of the circuit to claims about the MLE of the state at layer 1. [2 marks]

f) Using the techniques from the previous parts of the question, design an interactive proof to prove that $\mathcal{X}, \mathcal{Y} \in \mathbb{F}^{N \times N}$ satisfy $C(\mathcal{X}) = \mathcal{Y}$.

State and justify the communication complexity of your protocol in terms of elements of $\mathbb{F}$. [3 marks]