CS 355: Topics in Cryptography **Spring 2022**

Problem Set 4

Due: 5pm Friday, 20 May 2022 (submit via Gradescope)

Instructions: You **must** typeset your solution in LaTeX using the provided template:

`https://crypto.stanford.edu/cs355/22sp/homework.tex`

Submission Instructions: You must submit your problem set via Gradescope. Please use course code **862WDX** to sign up. Note that Gradescope requires that the solution to each problem starts on a **new page**.

Bugs: We make mistakes! If it looks like there might be a mistake in the statement of a problem, please ask a clarifying question on Ed.

Problem 1: True/False [4 points]. (one sentence explanation)

(a) Securely computing a function $f\colon \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ using Yao's protocol (as described in lecture), requires the two parties to exchange at most $O(n+m)$ bits in the worst case.

(b) You and your friends want to determine which one of you has the lowest salary. You design and run a protocol, at the end of which all your friends learn that their Big 4 salaries$^{\text{TM}}$ are higher than yours. This blatant invasion of your privacy could have been avoided if you had used a proper maliciously-secure MPC protocol.

Problem 2: Garbled Circuits are not maliciously secure [7 points]. Suppose that Alice has bit x, Bob has bit y, and they use Yao's GC protocol to compute $z = \text{AND}(x, y)$.

(a) (True/False, no explanation): If Alice's bit is 1, and all parties follow the protocol, then afterwards Alice can tell whether Bob's bit is 0 or 1.

(b) (True/False, no explanation): If Alice's bit is 0, and all parties follow the protocol, then afterwards Alice can tell whether Bob's bit is 0 or 1.

(c) Suppose that Alice has bit 0 and plays the role of the garbler. Show that by incorrectly garbling the circuit, and by observing the response of Bob (who is following the protocol), Alice can learn Bob's bit. Explicitly describe how Alice's attack works, and informally explain why Bob cannot detect that Alice has deviated from the protocol. In your attack, Alice *must* participate honestly in the OT protocol.

Problem 3: Compiling to R1CS [10 points]. The SNARG discussed in class ("Marlin") operates on relations expressed as rank-1 constraint systems (R1CSs). Recall that an R1CS instance comprises a set of variables, $\{v_1, \ldots v_n\}$ in a finite field $\mathbb{F}$, and constraints of the form $\left(a_0 + \sum_{i=1}^n a_i v_i\right)\left(b_0 + \sum_{i=1}^n b_i v_i\right) = c_0 + \sum_{i=1}^n c_i v_i$ where a_i, b_i, c_i are constants. Thus, each constraint requires the product of two linear combinations of variables (and the constant 1) to equal a third linear combination. Three examples with variables x, y, z: $xy = z$ is a rank-1 constraint that forces z to be the product of x and y; $0 = z - x - y$ is a

rank-1 constraint that forces z to be the sum of x and y; and $xxx = z$ is not a rank-1 constraint. For this problem, you may assume that the field has prime order.

To express relations defined in terms of booleans or fixed-width integers (like in C), these objects must be encoded as field element, and operations over them must be expressed as rank-1 constraints. In this problem, we'll consider booleans, encoded as $0 \in \mathbb{F}$ (false) or $1 \in \mathbb{F}$ (true). For a field element x which is bit-valued (zero or one), let $\mathsf{bool}(x)$ denote the corresponding boolean.

For each sub-problem you're given some inputs, assumptions that you can make about those inputs, and desired outputs. You should write the rank-1 constraints necessary to ensure that the outputs have the desired property. You may introduce auxiliary variables if needed.

Unless otherwise noted, each sub-problem requires only one or two constraints (you may use more if you wish). The first problem has been completed for you, as an example.

Extra Credit [2pts] Complete parts (a) through (g) in one constraint and parts (h) through (j) in two.

(a) **FORCE-BIT**: Given $x \in \mathbb{F}$, ensure is is bit-valued (there is no ouput).

Solution: The rank-1 constraint is: $(1-x)x = 0$.

(b) **NOT**: Given bit-valued $x \in \mathbb{F}$, ensure $r \in \mathbb{F}$ is bit-valued and $\mathsf{bool}(r) = \neg\mathsf{bool}(x)$.

(c) **AND**: Given bit-valued $x, y \in \mathbb{F}$, ensure $r \in \mathbb{F}$ is bit-valued and $\mathsf{bool}(r) = \mathsf{bool}(x) \wedge \mathsf{bool}(y)$.

(d) **OR**: Given bit-valued $x, y \in \mathbb{F}$, ensure $r \in \mathbb{F}$ is bit-valued and $\mathsf{bool}(r) = \mathsf{bool}(x) \vee \mathsf{bool}(y)$.

(e) **XOR**: Given bit-valued $x, y \in \mathbb{F}$, ensure $r \in \mathbb{F}$ is bit-valued and $\mathsf{bool}(r) = \mathsf{bool}(x) \oplus \mathsf{bool}(y)$.

(f) **BIT-EQUAL**: Given bit-valued $x, y \in \mathbb{F}$, ensure $r \in \mathbb{F}$ is bit-valued and $\mathsf{bool}(r) = \mathsf{bool}(x) \iff \mathsf{bool}(y)$.

(g) **FORCE-NON-ZERO**: Given $x \in \mathbb{F}$, ensure that is it non-zero (there is no output). Briefly explain why your constraints provide this guarantee.

Hint: you may want to introduce an auxiliary variable

(h) **IS-ZERO**: Given $x \in \mathbb{F}$ ensure $r \in \mathbb{F}$ is bit-valued and $\mathsf{bool}(r)$ is true iff x is zero. Briefly explain why your constraints provide this guarantee.

(i) **EQUAL**: Given $x, y \in \mathbb{F}$, ensure $r \in \mathbb{F}$ is bit-valued and $\mathsf{bool}(r)$ is true iff $x = y$. Briefly explain why your constraints provide this guarantee.

(j) **n-ary-AND** Given bit-values $x_1, \ldots, x_n \in \mathbb{F}$, ensure $r \in \mathbb{F}$ is bit-valued and $\mathsf{bool}(r) = \mathsf{bool}(x_1) \wedge \cdots \wedge \mathsf{bool}(x_n)$. Briefly explain why your constraints provide this guarantee.

You may assume that $n \ll |\mathbb{F}|$, and you may use only $O(1)$ constraints.

(k) [**Extra Credit (1pt)**] **n-ary-XOR** Given bit-values $x_1, \ldots, x_n \in \mathbb{F}$, ensure $r \in \mathbb{F}$ is bit-valued and $\mathsf{bool}(r) = \mathsf{bool}(x_1) \oplus \cdots \oplus \mathsf{bool}(x_n)$. Briefly explain why your constraints provide this guarantee.

You may assume that $n \ll |\mathbb{F}|$, and you may use only $O(\log n)$ constraints.

Problem 4: Verifiable Secret Sharing [10 points]. Consider a dealer who wants to share a secret α between n shareholders using the t-out-of-n Shamir secret-sharing scheme, for some $t < n$. The shareholders suspect that the dealer secretly holds a grudge against one of them and has given that person an invalid share, inconsistent with the rest of the shares. (We say that a set of shares is consistent if there exists a secret α such that every coalition of at least t shareholders can recover the (same) secret α.) In this problem, we assume that all shareholders are honest.

(a) Show that if they are willing to reveal all their shares, the shareholders can detect if one of them has indeed been given an invalid share.

We would like the shareholders to be able to detect an invalid share without having to reconstruct the secret in the verification process. To do this, consider the following modification to Shamir's secret-sharing scheme:

> Let $\mathbb{G}$ be a cyclic group of prime order $q > n$, and let g, h each be a generator of $\mathbb{G}$.
>
> 1. The dealer chooses $\beta, a_1, b_1, \ldots, a_{t-1}, b_{t-1} \xleftarrow{R} \mathbb{Z}_q$ and constructs the polynomials $A(x) = \alpha + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$ and $B(x) = \beta + b_1 x + b_2 x^2 + \cdots + b_{t-1} x^{t-1}$ over $\mathbb{Z}_q$.
> 2. The dealer creates t Pedersen commitments $c_0, c_1, \ldots, c_{t-1} \in \mathbb{G}$ where $c_o = \mathsf{Commit}(\alpha; \beta) = g^\alpha h^\beta$ and $c_j = \mathsf{Commit}(a_j; b_j) = g^{a_j} h^{b_j}$ for $j \in [t-1]$. The dealer publicly broadcasts all the commitments to all the shareholders.
> 3. The dealer creates n shares $\{(i, s_i, r_i)\}_{i=1}^n$, where $s_i = A(i)$ and $r_i = B(i)$ are computed over $\mathbb{Z}_q$. The dealer privately sends each of the n shareholders her own share.

(b) Describe a verification routine that allows the shareholders to jointly verify that all the shares given to them are valid without revealing any additional information about the secret.

(c) Prove that the protocol preserves the secrecy of the secret α against any coalition of fewer than t shareholders. [**Hint:** Specify the view of any coalition of $t-1$ shareholders and then prove this view is distributed independently of the secret α.]

(d) **Extra Credit [4 points].** Prove that if a dealer can trick the shareholders into accepting an invalid set of shares it can solve the disrete log of h with respect to g.

Problem 5: Generating Beaver Multiplication Triples [15 points]. Recall from lecture that Beaver multiplication triples enables general multiparty computation on secret-shared data. In this problem, we will explore two methods that can be used to generate Beaver multiplication triples. For simplicity, we will just consider the two-party setting and we will generate Beaver multiplication triples over the binary field $\mathbb{Z}_2$ (where addition corresponds to xor). To be precise, we first describe an "idealized process" for generating a single multiplication triple. In this "idealized process", a trusted party generates the triple and then distributes the shares of the triple to the two parties Alice and Bob.

1. The trusted party chooses $a, b \xleftarrow{R} \mathbb{Z}_2$ and computes $c = ab \in \mathbb{Z}_2$.

2. The trusted party distributes a 2-out-of-2 secret sharing of a, b, and c to Alice and Bob. Specifically, the trusted party samples $r_a, r_b, r_c \xleftarrow{R} \mathbb{Z}_2$ and gives r_a, r_b, r_c to Alice. The trusted party then computes $s_a = a \oplus r_a$, $s_b = b \oplus r_b$, and $s_c = c \oplus r_c$, and gives s_a, s_b, s_c to Bob.

By construction $[a] = (r_a, s_a)$ is an additive secret-sharing of a, $[b] = (r_b, s_b)$ is an additive secret-sharing of b, and $[c] = (r_c, s_c)$ is an additive secret-sharing of c. Moreover, $c = ab$, so $([a], [b], [c])$ is a valid Beaver multiplication triple.

We will show how Alice and Bob can generate these Beaver triples without relying on a trusted party. Throughout this problem, you may assume that Alice and Bob are "honest-but-curious" (namely, they follow the protocol exactly as described, but may try to infer additional information from the protocol transcript—this is the model that we considered in lecture).

(a) Show how Alice and Bob can generate a Beaver multiplication triple using Yao's protocol.[1] Your construction should not make any modifications to the internal details of Yao's protocol (in fact, any secure two-party computation protocol can be used here). Then, give an *informal* argument why your protocol is correct and secure. [**Hint:** To apply Yao's protocol, you will need to come up with a two-party functionality f that Alice and Bob will jointly compute. Try letting Alice's inputs to f be her shares (r_a, r_b, r_c), which she samples uniformly at random at the beginning of the protocol.]

(b) Show how Alice and Bob can use a *single invocation* of an 1-out-of-4 oblivious transfer (OT) protocol (on 1-bit messages) to generate a Beaver multiplication triple. Give an *informal* argument why your protocol is correct and secure. (In a 1-out-of-n OT, the sender has n messages $m_1, \ldots, m_n$, while the receiver has a single index $i \in [n]$. At the end of the protocol execution, the sender learns nothing while the receiver learns m_i (and nothing else). The formal definitions of sender and receiver privacy are the analogs of those presented in lecture.) [**Hint:** Try using OT to directly evaluate the functionality f you constructed from Part (a).]

(c) Let $\ell \in \mathbb{N}$ be a constant. Show how to build a 1-out-of-2^ℓ OT protocol (on 1-bit messages) using ℓ invocations of an 1-out-of-2 OT protocol (on λ-bit messages) together with a PRF $F\colon \{0,1\}^\lambda \times \{0,1\}^\ell \to \{0,1\}$. Here, $\{0,1\}^\lambda$ is the key-space of the PRF and $\{0,1\}^\ell$ is the domain of the PRF. Then, give an *informal* argument for why your protocol satisfies correctness, sender privacy, and receiver privacy. [**Hint:** Start by having the sender sample 2ℓ independent PRF keys. The sender will use these keys to blind each of its messages $m_1, \ldots, m_{2^\ell}$.]

[1] You may use the variant of Yao's protocol where only one party receives output (and the other party learns nothing).