CS 171: Discussion Section 12 (April 22)

1 Random Variables With a Linear Constraint

Let (A, B, C) be random variables with sample space $\mathbb{Z}_q$, and let $\alpha, \beta \in \mathbb{Z}_q \backslash \{0\}$ be fixed values. Consider the following three procedures for sampling (A, B, C):

1. Sample $A, B \leftarrow \mathbb{Z}_q$ independently and uniformly. Set
$$C = \alpha \cdot A + \beta \cdot B \mod q \tag{1.1}$$
2. Sample $B, C \leftarrow \mathbb{Z}_q$ independently and uniformly. Set
$$A = \frac{1}{\alpha}(C - \beta \cdot B) \mod q \tag{1.2}$$
3. Sample $A, C \leftarrow \mathbb{Z}_q$ independently and uniformly. Set
$$B = \frac{1}{\beta}(C - \alpha \cdot A) \mod q \tag{1.3}$$

Question: Prove that all three procedures sample (A, B, C) from the same distribution.

Claim 1.1. *Procedures 1, 2 and 3 sample (A, B, C) from the same distribution.*

Proof.

1. Intuition: Conditions 1.1, 1.2, and 1.3 are equivalent. (A, B, C) satisfy one of these conditions if and only if they satisfy the others.

   We have three variables and one linear constraint, so there are two degrees of freedom. Any pair of variables are uniformly distributed because there are two degrees of freedom, and the third variable is uniquely determined by the other two.

2. In Procedure 1: Given any values $a, b, c \in \mathbb{Z}_q$, we will compute $\Pr[A = a, B = b, C = c]$.

   If $c \neq \alpha \cdot a + \beta \cdot b \mod q$, then
$$\Pr[A = a, B = b, C = c] = 0$$
   Given that $A = a$ and $B = b$, the only value that C can take is $c = \alpha \cdot a + \beta \cdot b \mod q$.

   Next, if $c = \alpha \cdot a + \beta \cdot b \mod q$, then:
$$\begin{aligned}\Pr[A = a, B = b, C = c] &= \Pr_{A,B}[A = a, B = b] \cdot \Pr_{A,B}[C = c | A = a, B = b] \\ &= \Pr_A[A = a] \cdot \Pr_B[B = b] \cdot \Pr[C = \alpha \cdot a + \beta \cdot b \mod q | A = a, B = b] \\ &= \frac{1}{q} \cdot \frac{1}{q} \cdot 1 \\ &= \frac{1}{q^2}\end{aligned}$$
   In summary, in procedure 1,
$$\Pr[A = a, B = b, C = c] = \begin{cases} \frac{1}{q^2}, & \text{if } c = \alpha \cdot a + \beta \cdot b \mod q \\ 0, & \text{else} \end{cases}$$

3. In Procedures 2 and 3, we can also show that for any values $a, b, c \in \mathbb{Z}_q$,

$$\Pr[A = a, B = b, C = c] = \begin{cases} \frac{1}{q^2}, & \text{if } c = \alpha \cdot a + \beta \cdot b \mod q \\ 0, & \text{else} \end{cases}$$

   This follows a similar argument to the case of procedure 1. For the sake of completeness, we will give full proofs below for proceudres 2 and 3, but some readers may not need to read any further.

4. In procedure 2, we will compute $\Pr[A = a, B = b, C = c]$.

   First, if $c \neq \alpha \cdot a + \beta \cdot b \mod q$, then $a \neq \frac{1}{\alpha}(c - \beta \cdot b) \mod q$, so

$$\Pr[A = a, B = b, C = c] = 0$$

   Next, if $c = \alpha \cdot a + \beta \cdot b \mod q$, then:

$$\begin{aligned}\Pr[A = a, B = b, C = c] &= \Pr_{B,C}[B = b, C = c] \cdot \Pr_{B,C}[A = a | B = b, C = c] \\ &= \Pr_{B}[B = b] \cdot \Pr_{C}[C = c] \cdot \Pr\left[A = \frac{1}{\alpha}(c - \beta \cdot b) \mod q | B = b, C = c\right] \\ &= \frac{1}{q} \cdot \frac{1}{q} \cdot 1 \\ &= \frac{1}{q^2}\end{aligned}$$

5. In procedure 3, we will compute $\Pr[A = a, B = b, C = c]$.

   First, if $c \neq \alpha \cdot a + \beta \cdot b \mod q$, then $b \neq \frac{1}{\beta}(c - \alpha \cdot a) \mod q$, so

$$\Pr[A = a, B = b, C = c] = 0$$

   Next, if $c = \alpha \cdot a + \beta \cdot b \mod q$, then:

$$\begin{aligned}\Pr[A = a, B = b, C = c] &= \Pr_{A,C}[A = a, C = c] \cdot \Pr_{A,C}[B = b | A = a, C = c] \\ &= \Pr_{A}[A = a] \cdot \Pr_{C}[C = c] \cdot \Pr\left[B = \frac{1}{\beta}(c - \alpha \cdot a) \mod q | A = a, C = c\right] \\ &= \frac{1}{q} \cdot \frac{1}{q} \cdot 1 \\ &= \frac{1}{q^2}\end{aligned}$$

□

2 Schnorr Proof of Knowledge

The Schnorr protocol seen in lecture 17 allows a prover to prove that they know the discrete log of h. We will prove that it satisfies honest-verifier zero-knowledge, which means that if the verifier follows the protocol, then the protocol tells them nothing about $\log_g(h)$.

Inputs to the protocol: Let $(\mathbb{G}, q, g)$ be the parameters of a (cyclic) group of prime order q, let $h \in \mathbb{G} \backslash \{1\}$, and let $w \in \mathbb{Z}_q \backslash \{0\}$ be the unique value that satisfies $h = g^w$.

The verifier receives the following tuple x:

$$x = (\mathbb{G}, q, g, h)$$

and the prover receives (x, w). In the language of proof systems, x is the **instance** (the public input), and w is the **witness** (the prover's secret input).

Schnorr Protocol:

1. The prover samples $k \leftarrow \mathbb{Z}_q$ and sends $i := g^k$ to the verifier.
2. The verifier samples $r \leftarrow \mathbb{Z}_q$ and sends r to the prover.
3. The prover computes $s = r \cdot w + k \mod q$ and sends s to the verifier.
4. The verifier accepts if $g^s = h^r \cdot i$.

Question: Prove that this protocol satisfies completeness and honest-verifier zero-knowledge.

2.1 Completeness

Completeness says that the verifier will accept with overwhelming probability if both parties follow the protocol honestly.

Definition 2.1 (Completeness)**.** *The protocol satisfies **completeness** if when $h = g^w$ and the prover P and verifier V follow the protocol honestly, then*

$$\Pr[V \textit{ accepts}] \geq 1 - \mathsf{negl}(\lambda)$$

where λ is the security parameter.

2.2 Honest Verifier Zero-Knowledge

Intuitively, honest-verifier zero-knowledge (HVZK) says that the verifier should not learn any information about the secret w during an honest execution of the protocol. More formally, HVZK says that anything the verifier learns from the protocol (their view) can be simulated without knowledge of w.

In this protocol, the **view** of the honest verifier comprises the following variables:

$$\mathsf{view}(V; x, w) = (\mathbb{G}, q, g, h, i, r, s)$$

The view $\mathsf{view}(V; x, w)$ is a list of all of the verifier's inputs and any messages sent to and from the verifier.

The **simulator** Sim tries to simulate the view $\mathsf{view}(V; x, w)$ of the honest verifier, but Sim does not receive w as input. Sim does get x as input and gets to run V on any inputs of its choice.

The protocol satisfies **honest-verifier zero-knowledge** if there exists a simulator Sim that simulates the verifier's view in the honest protocol.

Definition 2.2 (Honest-Verifier Zero-Knowledge)**.** *The protocol satisfies **honest-verifier zero-knowledge** if there exists a simulator Sim such that if the protocol's inputs (x, w) satisfy $h = g^w$ and the prover and verifier follow the protocol honestly, then for any distinguisher D:*

$$\left| \Pr\left[D\big(\mathsf{view}(V; x, w)\big) \to 1 \right] - \Pr\left[D\big(\mathsf{Sim}^V(x)\big) \to 1 \right] \right| \leq \mathsf{negl}(\lambda)$$

where λ is the security parameter.

Claim 2.3. *The Schnorr protocol satisfies completeness.*

Proof. If the prover and verifier are honest, then $i = g^k$ and $s = r \cdot w + k \mod q$. Furthermore, we are given that $h = g^w$.

Next,

$$\begin{aligned} g^s = g^{r \cdot w + k} &= (g^w)^r \cdot g^k \\ &= h^r \cdot i \end{aligned}$$

So the verifier will accept with probability 1. □

Claim 2.4. *The Schnorr protocol satisfies honest-verifier zero-knowledge (HVZK).*

Proof.

1. To prove HVZK, we must construct a simulator for the view of the verifier.
   Construction of $\mathsf{Sim}^V(x)$:

   (a) Sample $r, s \leftarrow \mathbb{Z}_q$ independently and uniformly at random.

   (b) Compute $i = g^s \cdot h^{-r}$.

   (c) Output $(\mathbb{G}, q, g, h, i, r, s)$.

   Note: The simulator samples (r, s, i) in a different order from the real protocol, which samples i, then r, then s. This technique, of changing the order of sampling, is commonly used by zero-knowledge simulators.

2. Next, we will show that the output distribution of $\mathsf{Sim}^V(x)$ is identical to the distribution of $\mathsf{view}(V; x, w)$ in the honest protocol.

   In the description of $\mathsf{Sim}^V(x)$, we will define $k = \log_g(i)$. This is analogous to the k defined in the real protocol. Next, let (K, R, S) be the random variables that take values (k, r, s) respectively.

   In the real protocol, (K, R, S) have the following distribution: first $K, R \leftarrow \mathbb{Z}_q$ are sampled independently and uniformly at random. Then S is the unique value that satisfies:

   $$S = R \cdot w + K$$

   In the simulated protocol, $\mathsf{Sim}^V(x)$ samples (K, R, S) as follows: first, $R, S \leftarrow \mathbb{Z}_q$ are sampled independently and uniformly at random. Then K is the unique value that satisfies:

   $$K = S - R \cdot w$$

   By claim 1.1, the distribution of (K, R, S) is the same in the real protocol and in the simulated protocol.

3. Therefore, the output of $\mathsf{Sim}^V(x)$ is identical to the distribution of $\mathsf{view}(V; x, w)$ in the honest protocol.

Then for any distinguisher D:

$$\left| \Pr\left[D\big(\mathsf{view}(V; x, w)\big) \to 1 \right] - \Pr\left[D\big(\mathsf{Sim}^V(x)\big) \to 1 \right] \right| = 0$$

So the protocol satisfies honest-verifier zero-knowledge.

□