19.5 Sigma protocols: examples

So far, the only Sigma protocol we have seen is that of Schnorr, which allows a prover to convince a skeptical verifier that it "knows" the discrete logarithm of a given group element, without revealing anything about the discrete logarithm to the verifier. In this section, we present several additional examples of Sigma protocols. These examples not only serve to flesh out the general theory of Sigma protocols, they also have many practical applications, some of which we will discuss below.

19.5.1 Okamoto's protocol for representations

Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Let $h \in \mathbb{G}$ be some arbitrary group element. We will think of h for now as a system parameter — generated once and for all at system setup time, and publicly available to all parties. Recall (see Section 10.6.1) that for $u \in \mathbb{G}$, a representation of u (relative to g and h) is a pair $(\alpha, \beta) \in \mathbb{Z}_q^2$ such that $g^\alpha h^\beta = u$.

Okamoto's protocol allows a prover to convince a skeptical verifier that he "knows" a representation of a given $u \in \mathbb{G}$, without revealing anything about that representation to the verifier. More precisely, it is a Sigma protocol for the relation

$$\mathcal{R} = \left\{ \left((\alpha, \beta),\ u \right) \in \mathbb{Z}_q^2 \times \mathbb{G} :\ g^\alpha h^\beta = u \right\}. \tag{19.11}$$

A witness for the statement $u \in \mathbb{G}$ is $(\alpha, \beta) \in \mathbb{Z}_q^2$ such that $g^\alpha h^\beta = u$, i.e., a representation of u. Thus, in this example, every statement has many witnesses (precisely q, in fact).

The challenge space $\mathcal{C}$ for Okamoto's protocol is assumed to be a subset of $\mathbb{Z}_q$. The protocol (P, V) runs as follows, where the prover P is initialized with $((\alpha, \beta), u) \in \mathcal{R}$ and the verifier V is initialized with $u \in \mathbb{G}$:

1. P computes
$$\alpha_{\mathrm{t}} \xleftarrow{\mathrm{R}} \mathbb{Z}_q,\ \ \beta_{\mathrm{t}} \xleftarrow{\mathrm{R}} \mathbb{Z}_q,\ \ u_{\mathrm{t}} \leftarrow g^{\alpha_{\mathrm{t}}} h^{\beta_{\mathrm{t}}},$$
and sends the commitment u_{t} to V;

2. V computes $c \xleftarrow{\mathrm{R}} \mathcal{C}$, and sends the challenge c to P;

3. P computes
$$\alpha_{\mathrm{z}} \leftarrow \alpha_{\mathrm{t}} + \alpha c \in \mathbb{Z}_q,\ \ \beta_{\mathrm{z}} \leftarrow \beta_{\mathrm{t}} + \beta c \in \mathbb{Z}_q,$$
and sends the response $(\alpha_{\mathrm{z}}, \beta_{\mathrm{z}})$ to V;

4. V checks if $g^{\alpha_{\mathrm{z}}} h^{\beta_{\mathrm{z}}} = u_{\mathrm{t}} \cdot u^c$; if so V outputs accept; otherwise, V outputs reject.

See Fig. 19.6.

Theorem 19.9. *Okamoto's protocol is a Sigma protocol for the relation $\mathcal{R}$ defined in (19.11). Moreover, it provides special soundness and is special HVZK.*

Proof. Clearly, Okamoto's protocol has the required syntactic structure of a Sigma protocol. An accepting conversation for $u \in \mathbb{G}$ is of the form

$$(u_{\mathrm{t}}, c, (\alpha_{\mathrm{z}}, \beta_{\mathrm{z}})) \quad \text{such that} \quad g^{\alpha_{\mathrm{z}}} h^{\beta_{\mathrm{z}}} = u_{\mathrm{t}} \cdot u^c.$$

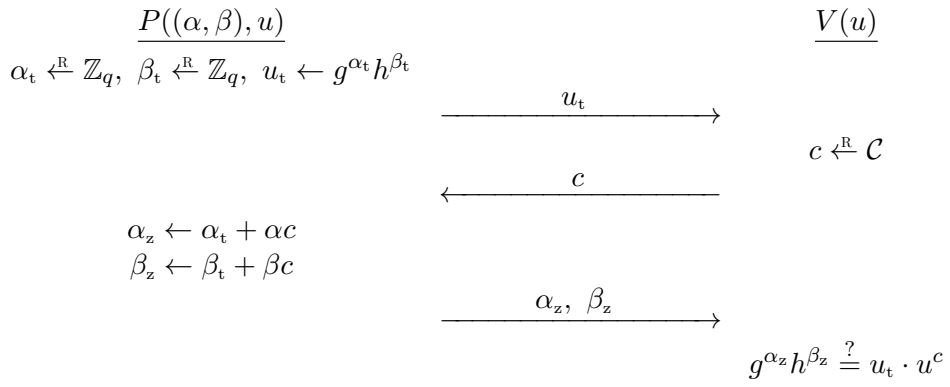

Figure 19.6: Okamoto's protocol

Correctness. We have to verify that the protocol satisfies the basic correctness requirement that an interaction between an honest prover and an honest verifier always produces an accepting conversation. This is easy to verify, since if

$$u_t = g^{\alpha_t} h^{\beta_t}, \quad \alpha_z = \alpha_t + \alpha c, \quad \text{and} \quad \beta_z = \beta_t + \beta c,$$

then we have

$$g^{\alpha_z} h^{\beta_z} = g^{\alpha_t + \alpha c} h^{\beta_t + \beta c} = g^{\alpha_t} h^{\beta_t} \cdot (g^{\alpha} h^{\beta})^c = u_t \cdot u^c.$$

Special soundness. Next, we show that Okamoto's protocol provides special soundness. Suppose we have two accepting conversations

$$(u_t, c, (\alpha_z, \beta_z)) \quad \text{and} \quad (u_t, c', (\alpha'_z, \beta'_z))$$

for the statement u, where $c \neq c'$. We have to show how to efficiently extract a representation of u from these two conversations. The computation here is very similar to that in Schnorr's protocol. Observe that

$$g^{\alpha_z} h^{\beta_z} = u_t \cdot u^c \quad \text{and} \quad g^{\alpha'_z} h^{\beta'_z} = u_t \cdot u^{c'},$$

and dividing the first equation by the second, the u_t's cancel, and we have

$$g^{\Delta\alpha} h^{\Delta\beta} = u^{\Delta c}, \quad \text{where } \Delta\alpha := \alpha_z - \alpha'_z, \ \ \Delta\beta := \beta_z - \beta'_z, \quad \Delta c := c - c'.$$

and so the witness extractor can efficiently compute a representation $(\alpha, \beta) \in \mathbb{Z}_q^2$ of u as follows:

$$\alpha \leftarrow \Delta\alpha / \Delta c, \quad \beta \leftarrow \Delta\beta / \Delta c.$$

Note that because $c \neq c'$, the value Δc is invertible in $\mathbb{Z}_q$. Here we use the fact that q is a prime.

Special HVZK. Finally, we show that Okamoto's protocol is special HVZK by exhibiting a simulator. Again, this is very similar to what we did for Schnorr's protocol. On input $u \in \mathbb{G}$ and $c \in \mathcal{C}$, the simulator computes

$$\alpha_z \xleftarrow{R} \mathbb{Z}_q, \ \ \beta_z \xleftarrow{R} \mathbb{Z}_q, \ \ u_t \leftarrow g^{\alpha_z} h^{\beta_z} / u^c,$$

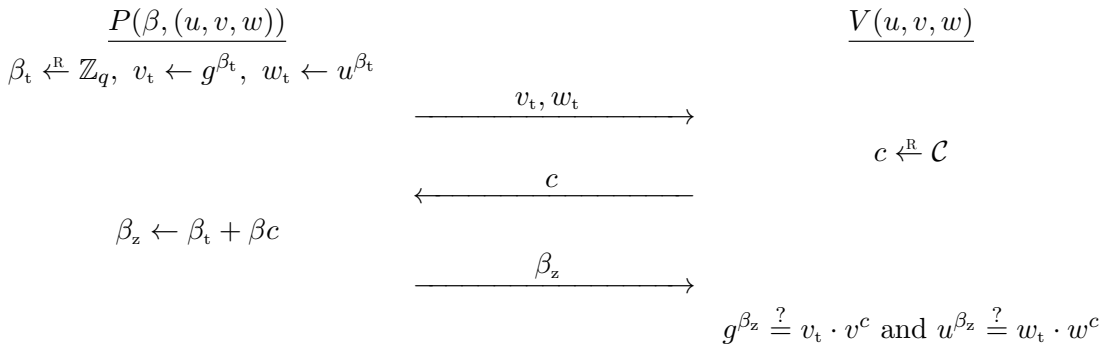

Figure 19.7: The Chaum-Pedersen protocol

---

and outputs $(u_t, (\alpha_z, \beta_z))$. Observe that the output always yields an accepting conversation, as required.

Now we argue that when $c \in \mathcal{C}$ is chosen at random, the output of the simulator on input u, c has the right distribution. The key observation is that in a real conversation, c, α_z, and β_z are mutually independent, with c uniformly distributed over $\mathcal{C}$, and α_z and β_z both uniformly distributed over $\mathbb{Z}_q$; moreover, given c, α_z, and β_z, the value u_t is uniquely determined by the equation

$$g^{\alpha_z} h^{\beta_z} = u_t \cdot u^c.$$

It should be clear that this is the same as the output distribution of the simulator. □

19.5.2 The Chaum-Pedersen protocol for DH-triples

The Chaum-Pedersen protocol allows a prover to convince a skeptical verifier that a given triple is a DH-triple, without revealing anything else to the verifier.

Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$, as usual. Recall (see Section 10.5) that for $\alpha, \beta, \gamma \in \mathbb{Z}_q$, we say that $(g^\alpha, g^\beta, g^\gamma)$ is a DH-triple if $\gamma = \alpha\beta$. Equivalently, (u, v, w) is a DH-triple if and only if there exists $\beta \in \mathbb{Z}_q$ such that $v = g^\beta$ and $w = u^\beta$.

The Chaum-Pedersen protocol is a Sigma protocol for the relation

$$\mathcal{R} := \left\{ \left(\beta,\ (u, v, w) \right) \in \mathbb{Z}_q \times \mathbb{G}^3 :\ v = g^\beta \text{ and } w = u^\beta \right\}. \tag{19.12}$$

A witness for the statement $(u, v, w) \in \mathbb{G}^3$ is $\beta \in \mathbb{Z}_q$ such that $v = g^\beta$ and $w = u^\beta$. Thus, a statement has a witness if and only if it is a DH-triple. Unlike the other examples we have seen so far, not all statements have a witness.

The Chaum-Pedersen protocol (P, V) is given in Fig. 19.7. The challenge space $\mathcal{C}$ is a subset of $\mathbb{Z}_q$.

Theorem 19.10. *The Chaum-Pedersen protocol is a Sigma protocol for the relation $\mathcal{R}$ defined in (19.12). Moreover, it provides special soundness and is special HVZK.*

Proof. The protocol has the required syntactic structure of a Sigma protocol. An accepting conversation for $(u, v, w) \in \mathbb{G}^3$ is of the form

$$((v_t, w_t), c, \beta_z) \quad \text{such that} \quad g^{\beta_z} = v_t \cdot v^c \text{ and } u^{\beta_z} = w_t \cdot w^c.$$

We leave it to the reader to verify that an interaction between an honest prover and an honest verifier always produces an accepting conversation.

Special soundness. Suppose we have two accepting conversations

$$((v_{\mathrm{t}}, w_{\mathrm{t}}), c, \beta_{\mathrm{z}}) \quad \text{and} \quad ((v_{\mathrm{t}}, w_{\mathrm{t}}), c', \beta'_{\mathrm{z}})$$

for the statement (u, v, w), where $c \neq c'$. The reader may verify that

$$\beta := \Delta\beta / \Delta c, \quad \text{where } \Delta\beta := \beta_{\mathrm{z}} - \beta'_{\mathrm{z}},\ \Delta c := c - c',$$

is the corresponding witness.

Special HVZK. On input $(u, v, w) \in \mathbb{G}^3$ and $c \in \mathcal{C}$, the simulator computes

$$\beta_{\mathrm{z}} \xleftarrow{\mathrm{R}} \mathbb{Z}_q, \ \ v_{\mathrm{t}} \leftarrow g^{\beta_{\mathrm{z}}} / v^c, \ \ w_{\mathrm{t}} \leftarrow u^{\beta_{\mathrm{z}}} / w^c.$$

and outputs $((v_{\mathrm{t}}, w_{\mathrm{t}}), \beta_{\mathrm{z}})$. Observe that the output always yields an accepting conversation, as required.

Now we argue that when $c \in \mathcal{C}$ is chosen at random, the output of the simulator on input $((u, v, w), c)$ has the right distribution. The key observation is that in a real conversation, c and β_{z} are independent, with c uniformly distributed over $\mathcal{C}$ and β_{z} uniformly distributed over $\mathbb{Z}_q$; moreover, given c and β_{z}, the values v_{t} and w_{t} are uniquely determined by the equations

$$g^{\beta_{\mathrm{z}}} = v_{\mathrm{t}} \cdot v^c \text{ and } u^{\beta_{\mathrm{z}}} = w_{\mathrm{t}} \cdot w^c.$$

It should be clear that this is the same as the output distribution of the simulator. □

19.5.3 A Sigma protocol for arbitrary linear relations

The reader may have noticed a certain similarity among the Schnorr, Okamoto, and Chaum-Pedersen protocols. In fact, they are all special cases of a generic Sigma protocol for proving linear relations among group elements.

As usual, let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. We shall consider boolean formulas ϕ of the following type:

$$\phi(x_1, \ldots, x_n) \ \ := \ \ \left\{ \prod_{j=1}^{n} g_{1j}^{x_j} = u_1 \ \ \wedge \ \ \cdots \ \ \wedge \ \ \prod_{j=1}^{n} g_{mj}^{x_j} = u_m \right\}. \tag{19.13}$$

In such a formula ϕ, the g_{ij}'s and u_i's are elements of the group $\mathbb{G}$. Some of these group elements could be system parameters or even constants, while others are specific to the formula. The x_i's are the formal variables of the formula. When we assign values in $\mathbb{Z}_q$ to the variables $x_1, \ldots, x_n$, the formula evaluates to true if all the equalities in (19.13) hold.

For a specific class $\mathcal{F}$ of such formulas, we can define the relation

$$\mathcal{R} := \left\{ \ (\alpha_1, \ldots, \alpha_n), \ \phi \ \right) \in \mathbb{Z}_q^n \times \mathcal{F} : \ \phi(\alpha_1, \ldots, \alpha_n) = \text{true} \ \right\}. \tag{19.14}$$

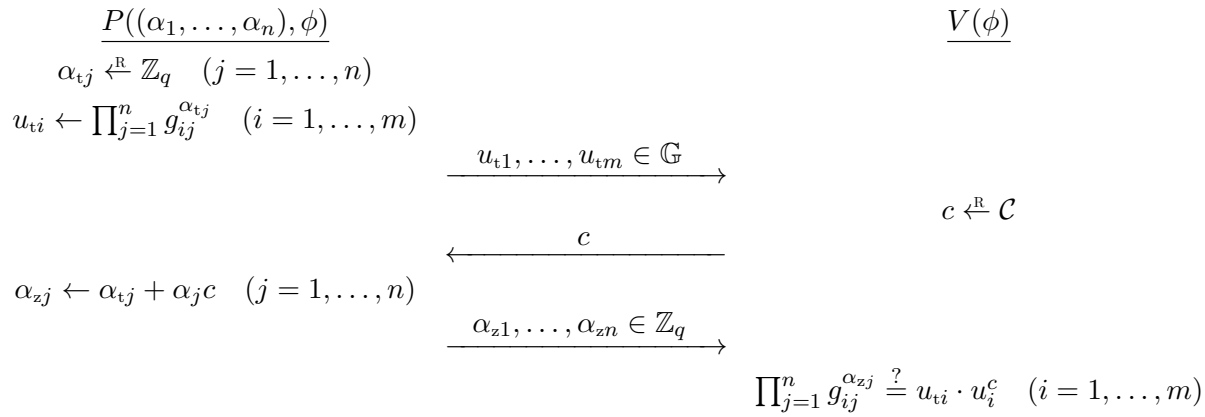

Figure 19.8: The generic linear protocol

So a statement is a formula $\phi \in \mathcal{F}$, and a witness for ϕ is an assignment $(\alpha_1,\ldots,\alpha_n) \in \mathbb{Z}_q^n$ to the variables $x_1,\ldots,x_n$ that makes the formula true. The reason we call this a set of "linear" relations is because if we take discrete logarithms, (19.13) can be written as the system of linear equations

$$\mathsf{Dlog}_g(u_i) = \sum_{j=1}^{n} x_j \cdot \mathsf{Dlog}_g(g_{ij}) \qquad \text{for } i = 1,\ldots,m.$$

A witness is a solution to this system of equations.

The **generic linear protocol** (P,V) for such a relation $\mathcal{R}$ is given in Fig. 19.8. The prover has ϕ and a witness $(\alpha_1,\ldots,\alpha_n) \in \mathbb{Z}_q^n$. As usual, the challenge space $\mathcal{C}$ is a subset of $\mathbb{Z}_q$. All the Sigma protocols presented so far are special cases of the generic linear protocol:

- Schnorr's protocol is a special case with $\phi_1(x) := \{u = g^x\}$.
- Okamoto's protocol is a special case with $\phi_2(x,y) := \{u = g^x h^y\}$.
- The Chaum-Pedersen protocol is a special case with $\phi_3(x) := \{v = g^x \ \wedge \ w = u^x\}$.

One can prove the following theorem by mimicking the proofs of the corresponding theorems for Schnorr, Okamoto, and Chaum-Pedersen. We leave it as an exercise for the reader.

Theorem 19.11. *The generic linear protocol in Fig. 19.8 is a Sigma protocol for the relation $\mathcal{R}$ defined in (19.14). Moreover, it provides special soundness and is special HVZK.*

We can generalize the generic linear protocol even further, where we allow the various equations in (19.13) to be over different groups. The only requirement is that all groups have the same prime order q. The protocol is exactly the same. A typical situation that arises in applications is where there are two types of equations: the first type are equations over a cryptographically interesting group $\mathbb{G}$ of order q, and the second type are equations over $\mathbb{Z}_q$, which are of the form $\kappa_i = \sum_{j=1}^{n} \lambda_{ij} x_j$, where the κ_i's and λ_{ij}'s are elements of $\mathbb{Z}_q$.

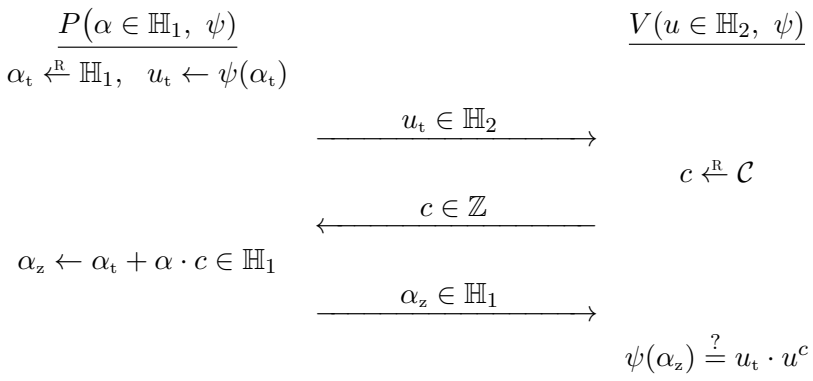

Figure 19.9: A Sigma protocol for the preimage of a homomorphism

19.5.4 A Sigma protocol for the pre-image of a homomorphism

All the Sigma protocols presented so far, including the general linear protocol, can be described more clearly and succinctly using the language of group homomorphisms. Let $\mathbb{H}_1$ and $\mathbb{H}_2$ be two finite abelian groups of known order and let $\psi : \mathbb{H}_1 \to \mathbb{H}_2$ be a group homomorphism. We will write the group operation in $\mathbb{H}_1$ additively and the group operation in $\mathbb{H}_2$ multiplicatively.

Let $u \in \mathbb{H}_2$. Fig. 19.9 gives a Sigma protocol that allows a prover to convince a verifier that it "knows" a preimage of u under ψ. Specifically, the protocol is a Sigma protocol for the relation

$$\mathcal{R} := \big\{\big(\alpha, (u, \psi)\big) \in \mathbb{H}_1 \times (\mathbb{H}_2 \times \mathcal{F}) :\ \psi(\alpha) = u\big\}. \tag{19.15}$$

Here $\alpha \in \mathbb{H}_1$ is the preimage under ψ for $u \in \mathbb{H}_2$. The prover in Fig. 19.9 has the witness $\alpha \in \mathbb{H}_1$, the verifier has the image $u \in \mathbb{H}_2$, and both parties have $(\mathbb{H}_1, \mathbb{H}_2, \psi)$. The challenge space $\mathcal{C}$ is $\{0, 1, \ldots, N-1\} \subseteq \mathbb{Z}$ for some integer N.

Let us see how this protocol encompases all the example Sigma protocols so far. Let $\mathbb{G}$ be a group of prime order q with generators $g, h, u \in \mathbb{G}$.

- Okamoto's protocol is a special case with $\mathbb{H}_1 := \mathbb{Z}_q^2$, $\mathbb{H}_2 := \mathbb{G}$, and $\psi_1(x, y) := g^x h^y$.
- The Chaum-Pedersen protocol is a special case with

  $$\mathbb{H}_1 := \mathbb{Z}_q, \quad \mathbb{H}_2 := \mathbb{G}^2, \quad \text{and} \quad \psi_2(x) := (g^x, u^x).$$

  We can even set $\mathbb{H}_2 := \mathbb{G}_1 \times \mathbb{G}_2$ with $g \in \mathbb{G}_1$, $u \in \mathbb{G}_2$, and $|\mathbb{G}_1| = |\mathbb{G}_2|$. Then for a given $(v, w) \in \mathbb{G}_1 \times \mathbb{G}_2$, proving knowledge of a ψ_2 preimage of (v, w) proves equality of discrete-logs $\mathsf{Dlog}_g(v) = \mathsf{Dlog}_u(w)$ in distinct groups $\mathbb{G}_1$ and $\mathbb{G}_2$.
- The general linear protocol in Fig. 19.8 is a special case with

  $$\mathbb{H}_1 := (\mathbb{Z}_q)^n, \quad \mathbb{H}_2 := \mathbb{G}^m, \quad \text{and} \quad \psi_3(x_1, \ldots, x_n) := \left(\prod_{j=1}^{n} g_{1j}^{x_j}, \ \ldots, \ \prod_{j=1}^{n} g_{mj}^{x_j} \right).$$

  where $g_{ij} \in \mathbb{G}$ for all $i = 1, \ldots, m$ and $j = 1, \ldots, n$.

One can easily verify that the maps ψ_1, ψ_2, ψ_3 are group homomorphims. By using these homomorphims in the protocol of Fig. 19.9 we obtain all the example protocols in this section as a special case.

Theorem 19.12. *The protocol in Fig. 19.9 is a Sigma protocol for the relation $\mathcal{R}$ defined in (19.15). Moreover, it is special HVZK, and provides special soundness whenever the smallest prime factor of $|\mathbb{H}_1| \times |\mathbb{H}_2|$ is at least $|\mathcal{C}|$.*

The proof exactly mimicks the proof of the corresponding theorem for the Schnorr protocol. We require the lower bound on the smallest prime factor of $|\mathbb{H}_1| \times |\mathbb{H}_2|$ to ensure that the witness extractor can obtain a ψ preimage from two accepting conversations $(u_{\text{t}}, c, \alpha_{\text{z}})$ and $(u_{\text{t}}, c', \alpha'_{\text{z}})$. As in the witness extractor for the Schnorr protocol, we obtain a relation $\psi(\Delta\alpha) = u^{\Delta c}$ where $\Delta\alpha := (\alpha_{\text{z}} - \alpha'_{\text{z}}) \in \mathbb{H}_1$ and $\Delta c := (c - c') \in \mathbb{Z}$. The lower bound on the prime factors of $|\mathbb{H}_1|$ and $|\mathbb{H}_2|$ ensures that (1) we can divide $\Delta\alpha$ by Δc in $\mathbb{H}_1$, and (2) we can take a Δc root of the right hand side by raising it to the power of $((\Delta c)^{-1} \bmod |\mathbb{H}_2|) \in \mathbb{Z}$. We then obtain the relation $\psi(\Delta\alpha/\Delta c) = u$ so that $\Delta\alpha/\Delta c \in \mathbb{H}_1$ is a preimage of $u \in \mathbb{H}_2$ under ψ, as required.

19.5.5 A Sigma protocol for RSA

Lest the reader think that Sigma protocols are only for problems related to discrete logarithms, we present one related to RSA.

Let (n, e) be an RSA public key, where e is a prime number. We will view (n, e) as a system parameter. The Guillou-Quisquater (GQ) protocol allows a prover to convince a skeptical verifier that he "knows" an eth root of $y \in \mathbb{Z}_n^*$, without revealing anything else. More precisely, it is a Sigma protocol for the relation

$$\mathcal{R} = \left\{ (x, y) \in \mathbb{Z}_n^* \times \mathbb{Z}_n^* : \ x^e = y \right\}. \tag{19.16}$$

A witness for a statement $y \in \mathbb{Z}_n^*$ is $x \in \mathbb{Z}_n^*$ such that $x^e = y$. Since (n, e) is an RSA public key, the map that sends $x \in \mathbb{Z}_n^*$ to $y = x^e \in \mathbb{Z}_n^*$ is bijective. Therefore, every statement has a unique witness.

The GQ protocol (P, V) is given in Fig. 19.10. The challenge space $\mathcal{C}$ is a subset of $\{0, \ldots, e-1\}$. Notice that when e is small, the challenge space is small. If needed, it can be enlarged using the method of Exercise 19.6. However, when using this protocol we will typically ensure that the challenge space is large by taking e to be a large prime.

The GQ protocol in Fig. 19.10 is a special case of the protocol in Fig. 19.9 for proving knowledge of the preimage of a homomorphism. Here the homomorphism is $\psi : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ defined by $\psi(x) = x^e$. However, special soundness does not follow from Theorem 19.12 because the group $\mathbb{Z}_n^*$ has unknown order. Instead, we have to give a seperate proof of these properties. We do so in the following theorem.

Theorem 19.13. *The GQ protocol is a Sigma protocol for the relation $\mathcal{R}$ defined in (19.16). Moreover, it provides special soundness and is special HVZK.*

Proof. An accepting conversation for y is of the form $(x_{\text{t}}, c, x_{\text{z}})$, where $x_{\text{z}}^e = y_{\text{t}} \cdot y^c$. The reader may easily verify the basic correctness requirement: an interaction between an honest prover and an honest verifier always produces an accepting conversation.