**Schnorr protocol**

One of the simplest and frequently used proofs of knowledge, the *proof of knowledge of a* [*discrete logarithm*](http://en.wikipedia.org/wiki/Discrete_logarithm), is due to Schnorr.[[3]](http://en.wikipedia.org/wiki/Proof_of_knowledge#cite_note-2) The protocol is defined for a [cyclic group](http://en.wikipedia.org/wiki/Cyclic_group) *Gq* of order *q* with generator *g*.

In order to prove knowledge of *x* = log*gy*, the prover interacts with the verifier as follows:

1. In the first round the prover commits herself to randomness *r*; therefore the first message *t* = *gr* is also called *commitment*.
2. The verifier replies with a *challenge* *c* chosen at random.
3. After receiving *c*, the prover sends the third and last message (the *response*) *s* = *r* + *cx*.

The verifier accepts, if *gs* = *tyc*.

**Sigma protocols**

Protocols which have the above three move structure: commitment, challenge and response, are called sigma protocols. The Greek Σ visualizes the flow of the protocol. Sigma protocols exist for proving various statements, such as those pertaining to discrete logarithms. Using these proofs, the prover can not only prove the knowledge of the discrete logarithm but also that the discrete logarithm is of a specific form. For instance it is possible to prove that two logarithms of *y*1 and *y*2 with respect to bases *g*1 and *g*2 are equal or fulfill some other [linear](http://en.wikipedia.org/wiki/Linear) [relation](http://en.wikipedia.org/wiki/Relation_%28mathematics%29). For *a* and *b* elements of *Zq*, we say that the prover proves knowledge of *x*1 and *x*2 such that y_1= g_1^{x_1} \land y_2=g_2^{x_2}and *x*2 = *ax*1 + *b*. Equality corresponds to the special case where *a* = 1 and *b* = 0. As *x*2 can be [trivially](http://en.wikipedia.org/wiki/Trivial_%28mathematics%29) computed from *x*1 this is equivalent to proving knowledge of an *x* such thaty_1= g_1^{x} \land y_2={(g_2^a)}^{x} g_2^b.

This is the intuition behind the following notation, which is commonly used to express what exactly is proven by a proof of knowledge.

PK\{(x): y_1= g_1^{x} \land y_2={(g_2^a)}^{x} g_2^b \},

states that the prover knows an *x* that fulfills the relation above.