# 19 GUILLOU-QUISQUATER ZERO KNOWLEDGE TRANSFER IDENTIFICATION PROTOCOL

### Security of Guillou-Quisquater Protocol

Extracting $b^{th}$ roots modulo the composite integer $n$ is necessary to defeat the protocol; this is no harder than factoring $n$, which we already know to be computationally intractable.

## Comparison of Fiat-Shamir, Schnorr and Guillou-Quisquater Protocols

Each of these protocols provides solutions to the identification problem. Each has relative advantages and disadvantages with respect to various performance criteria and for specific applications.Each protocol can be compared under the following criteria:

2. *Offline computations*

   The Schnorr scheme has the advantage of requiring only a single online modular multiplication by the claimant. This assumes (as outlined earlier) that the exponentiation is done beforehand. However, significant computations is required by the verifier (Bob) compared to the Fiat-Shamir or GQ scheme.

3. *Security assumptions*

All the protocols require the assumptions that the following problems are intractable:

For a composite integer $n$:

Fiat-Shamir – extracting square roots mod $n$

Schnorr – computing discrete logs mod a prime number $p$.

Guillou-Quisquater – extracting $b^{th}$ roots mod $n$

Encryption can be expressed by the equations:

$$D = \left(r \times G^{d}\right) \bmod n \tag{1}$$

Decryption can be expressed by the equations:

$$T' = \left(D^{V} I^{d}\right) \bmod n. \tag{2}$$