# The Guillou-Quisquater Protocol (GQ)

January 29, 2011

The GQ protocol allows $\mathcal{P}$ to prove to $\mathcal{V}$ that she knows the $e-$th root $w$ modulo $n$ of a given number $y \in \mathbb{Z}_n$.
The protocol works as follows:

1. $\mathcal{P}$ chooses $t \in \mathbb{Z}_n^*$ at random and sends the group element $u = t^e \mod n$ to $\mathcal{V}$
2. $\mathcal{V}$ chooses the challenge value $c \in \{0, \ldots, e-1\}$
3. $\mathcal{P}$ answers by sending the value $s = t \cdot w^c$ and $\mathcal{V}$ accepts if and only if $s^e = u \cdot y^c$

Define

$$R_{RSA} = \{(x, w) : x = (u, e, y),\ w = y^{\frac{1}{e}} \mod n\}^1$$

We show the three basic properties of the Zero Knowledge Proofs of Knowledge, i.e. Completeness, Soundness and Zero Knowledge:

**Completeness:** It suffices to show that if $x \in \mathcal{L}$ and $R(x, w) = 1$ for some witness $w$, then for all strings $z$

$$\mathsf{Prob}[\mathsf{out}^{\mathcal{V}}_{\mathcal{P},\mathcal{V}}(x, w, z) = 1] = 1$$

It is easy to see that

$$s^e = (tw^c)^e = t^e(w^e)^c$$

and

$$uy^c = t^e(w^e)^c$$

**Soundness:** We need to show that for every convincing prover $\mathcal{P}^*$ there exists a knowledge extractor $K$ such that on $\mathcal{P}^*$'s input it extracts a $w$ for $x$.

Firstly we see how we can obtain two accepting conversations from $\mathcal{P}^*$ with challenge values $c,\ c^*$ such that $c \neq c^*$:

Let two conversations with $\mathcal{P}^*$, that share the same first move, $(u, c, s)$ and $(u, c^*, s^*)$. Then from the first conversation we have that

$$s^e = uy^c \tag{1}$$

and from the second we get

$$(s^*)^e = uy^{c^*} \tag{2}$$

[1] as opposed to $R_{DLOG} = \{(x, w) : x = (G, g, m.h),\ w = \log_g h\}$ that we used in Schnorr's Protocol

Combining (1) and (2) we have that

$$\left(\frac{s}{s^*}\right)^e = y^{c-c^*}$$

and using Euclid's extended gcd algorithm we can find $a$ and $b$ such that

$$ae + b(c - c^*) = 1$$

Then define

$$z = \left(\frac{s}{s^*}\right)^b y^a$$

then we have that

$$z^e = \left(\frac{s}{s^*}\right)^{be} y^{ae} = y^{(c-c^*)b} y^{ae} = y$$

Following the same methodology that was used in class to prove the soundness property for Schnorr's protocol, we first view $\mathcal{P}$ as a probabilistic program in two steps:

1. $\mathcal{P}(\mathsf{first}, \langle e, n\rangle,\ y)$ outputs $\langle u, \mathsf{aux}\rangle$
2. $\mathcal{P}(\mathsf{second},\ \langle e, n\rangle,\ c,\ \mathsf{aux})$ outputs $s$

where aux represents the internal information used by $\mathcal{P}$ and that is not published.

Now we develop a Knowledge Extractor with the following structure:

1. Let $\rho_1 \overset{R}{\leftarrow} \{0,1\}^{\lambda_1}$ be the coin tosses required by the first step of $\mathcal{P}$. Fix the randomness of $\mathcal{P}$ with $\rho_1$ and simulate $\mathcal{P}(\mathsf{first}, \langle e, n\rangle,\ y)$ to obtain $u$.
2. Choose $c \overset{R}{\leftarrow} \mathbb{Z}_n$
3. Let $\rho_2 \overset{R}{\leftarrow} \{0,1\}^{\lambda_2}$ be the coin tosses required by step 2 of $\mathcal{P}$. Simulate $\mathcal{P}(\mathsf{second},\ \langle e, n\rangle,\ c,\ \mathsf{aux})$ with fixed randomness $\rho_2$ to obtain $s$
4. Choose $c^* \overset{R}{\leftarrow} \mathbb{Z}_n$, $\rho_2^* \overset{R}{\leftarrow} \{0,1\}^{\lambda_2}$. Repeat steps 2 and 3 to obtain $s^*$ and output $\langle u, c, s\rangle$ and $\langle u, c^*, s^*\rangle$

So using the above technique, the knowledge extractor cat obtain two accepting conversations and reconstruct the witness as previously discussed. We will now show that the knowledge extractor can produce the two accepting conversations with adequate probability.

Suppose that the prover is successful with at least non negligable probability $\alpha$. Let

$$X \times Y = \left\{(\rho_1, (c, \rho_2)) : \rho_1 \in \{0,1\}^{\lambda_1},\ (c, \rho_2) \in \mathbb{Z}_n \times \{0,1\}^{\lambda_2}\right\}$$

and define $A$ be the set of $(\rho_1, (c, \rho_2))$ that the verifier accepts. Then $|A| \geq \alpha|X \times Y|$. Then we can fix a good sequence $(\rho_1, (c, \rho_2))$ in $A$ such that the resulting conversation from $K$ is accepting. By the Splitting Lemma, $K$ hits a super-good sequence in steps 1 to 3 with probability $\alpha/2$.

Suppose the knowledge extractor hits a super-good sequence. Then there is an $\alpha/2$ probability that $K$ hits another super-good sequence when repeating step 4. So the probability that both conversations are accepting is $\alpha^2/4$. Moreover, there is a $1/e$ probability that $K$ will generate the same challenge values $c = c^*$, which implies that for the property of Soundness to be valid in this protocol, $e$ needs to be sufficiently large.

Now let $S$ be the event that the knowledge extractor is successful, $C$ the event that $c \neq c^*$ in the second choice, $D$ the event that the sequence $(\rho_1, (c, \rho_2))$ is super-good and $E$ the event that the sequence $(\rho_1, (c^*, \rho_2^*))$ is good. Then

$$\mathsf{Prob}[S] \geq \mathsf{Prob}[C \wedge D \wedge E] = \mathsf{Prob}[D \wedge E] - \mathsf{Prob}[\neg C] = \frac{\alpha^2}{4} - \frac{1}{e}$$

which proves the soundness property for the GQ protocol.

**Zero Knowledge:** In order to prove the Zero Knowledge property we must show that for every verifier $\mathcal{V}^*$ there exists some simulator $S$ such that for every $x, w$ the following holds:

$$\Delta[S(x,z), \mathsf{out}_{\mathcal{P},\mathcal{V}^*}^{\mathcal{V}^*}(x,w,z)] = \mathsf{negl}$$

First we define the simulator $S$:
On input $(u, e, y)$, $S$ selects $c \overset{R}{\leftarrow} \{0, \ldots, e\}$ and $s \overset{R}{\leftarrow} \mathbb{Z}_n$ and outputs $(sy^{-c}, c, s)$

A real conversation is of the form

$$\mathsf{out}_{\mathcal{P},\mathcal{V}^*}^{\mathcal{V}^*}(x,w,z) = (t^e, c, tw^c)$$

and so we see that

$$\begin{aligned}\Big|\mathsf{Prob}[\mathcal{A}(S(x,z) = 1)] - \mathsf{Prob}[\mathcal{A}(\mathsf{out}_{\mathcal{P},\mathcal{V}^*}^{\mathcal{V}^*}(x,w,z)) = 1]\Big| &\leq \Delta[S(x,z), \mathsf{out}_{\mathcal{P},\mathcal{V}^*}^{\mathcal{V}^*}] \\ &\leq \left|\frac{1}{e \cdot n} - \frac{1}{e \cdot n}\right| \\ &= 0\end{aligned}$$