Handout 7: Solution for PS2, problem 2

Instructor: Anna Lysyanskaya *Teaching Assistant: Moses Liskov*

In the previous solution set, the solution for problem 2 was a partial one. The solution below is more complete and deals with a very tricky, very technical issue. Basically, in order to pump up the accuracy of our reduction we have to use the given adversary repeatedly. However, for this to actually increase the probability of success, we need to make the trials completely independent, by providing each trial with independent random input. Unfortunately, though we can provide independent random coins and random x and c (the dedicated QNR from the public key and the query ciphertext), we can't usefully give a random n each time. Fortunately, we can deal with this issue.

Problem 2

Prove that if for any $0 < q \leq 1/2$, the Goldwasser-Micali cryptosystem is q-GM-secure, then it is GM-secure.

Solution: We will prove this by proving the contrapositive. Suppose the Goldwasser-Micali cryptosystem (G, E, D) is not GM-secure. Then, there is an adversary that breaks it. And, by the reduction given in lecture, there is an algorithm $\{A_n\}$ such that for infinitely many k, there is some polynomial p such that

$$\Pr[n \leftarrow RSAM(k); a \leftarrow J_1(n); b \leftarrow A_k(x, n) : b = QC(x, pq)] > 1/2 + 1/p(k)$$

That is, $\{A_n\}$ solves the quadratic residuosity problem. We wish to construct an algorithm that breaks q-GM security. We do this as follows. We assume A'_k knows some polynomials ϕ and ψ.

$A'_k((n, x), c)$:

1. For $i = 1$ to $\psi(k)$ do:
   a. Select $r \leftarrow \mathbb{Z}_n^*$.
   b. Select $b \leftarrow \{0, 1\}$.
   c. Compute $b' = A_k(n, r^2 x^b)$.
   d. Record an "n is good" vote if $b' = b$.
2. If there are fewer than $(1/2 + 1/4\phi(k))\psi(k)$ "n is good" votes, output 1.
3. For $i = 1$ to $\psi(k)$ do:
   a. Select $r \leftarrow \mathbb{Z}_n^*$.
   b. Select $b \leftarrow \{0, 1\}$.
   c. Compute $b' = A_k(n, cr^2 x^b)$.
   d. Record one $\overline{b'} \oplus b$ vote.
4. Output whichever of 0 or 1 has more votes.

It is easy to verify that if A_k is correct when it outputs b' on input (n, cr^2x^b) then the correct answer is $\overline{b'} \oplus b$.

Basically, in step 1 the algorithm tests to see if A_k is good at the quadratic residuosity problem if n is fixed at the value we are given. If A_k is good, we use it repeatedly to get a high level of certainty about the answer. If A_k is not good, we basically are getting no help from A_k so we might as well just guess the most likely correct answer, namely 1 (since $q \leq 1/2$). Let $S_{q-GM}(k, A')$ be the event that

$$((n,x), SK) \leftarrow G(1^k); b \leftarrow \{q : 0, 1\}; c \leftarrow E(n, x, b); b' \leftarrow A'(n, x, c) : b' = b,$$

And let $P = \Pr[S_{q-GM}(k, A')]$. Say that n is "ϕ-good" if

$$\Pr[y \leftarrow J_1(n); b \leftarrow A_k(n, y) : b = QC(y, n)] \geq \frac{1}{2} + \frac{1}{2\phi(k)}$$

Let $\gamma(\phi, n)$ be the event that n is good, and let $P_\gamma = \Pr[n \leftarrow RSAM(k) : \gamma(\phi, n)]$. Now, let's assume for the moment that if n is good, we always use steps 3 and 4 to output our answer and if n is not good, we output 1. Then,

$$P = P_\gamma \Pr[S_{q-GM}(k, A') | \gamma(\phi, n)] + (1 - P_\gamma)(1 - q)$$

where ϕ is the same in $\gamma(\phi, n)$ and in the algorithm run by A'.

Theorem 1 *If $P_\gamma \geq 1/p(k)$ for some polynomial p, then for large enough $g(k)$, $P \geq 1 - q + 1/p'(k)$ for some nonnegligible function $1/p'$ and sufficiently large k.*

Proof. The basic idea here is that if there are a polynomial fraction of good n, and we always get the advantage the adversary provides on those n, then we will have enough of an advantage to break q-GM security. To prove this, we prove that $\Pr[S_{q-GM}(k, A') | \gamma(n)] \geq 1 - 2^{-k}$. If n is good, and we use steps 3 and 4 to output our answer, we have a probability of about $(1 - 1/\phi(k))^{\psi(k)}$, which for sufficiently large ψ is at least $1 - 2^{-k}$.

Now,

$$\begin{aligned} P &\geq \frac{1}{p(k)}(1 - 2^{-k}) + \left(1 - \frac{1}{p(k)}\right)(1 - q) \\ &= \frac{1 - 2^{-k}}{p(k)} + 1 - q - \frac{1 - q}{p(k)} \\ &= 1 - q + \frac{q - 2^{-k}}{p(k)} \\ &= 1 - q + \frac{1}{p'(k)}, \end{aligned}$$

where $p'(k) = p(k)/(q - 2^{-k})$. For sufficiently large k, $q > 2^{-k}$, so for such k, $1/p'(k)$ is a positive function which is nonnegligible, since it approaches $p(k)/q$ as k goes to infinity. □

Theorem 2 *$P_\gamma \geq 1/p(k)$ for some polynomial p.*

Proof. Define $S_{QR}(k, A)$ to be the event

$$n \leftarrow RSAM(k); c \leftarrow J_1(n); b \leftarrow A(n, c) : b = QC(n, c).$$

Now, we know that $\Pr[S_{QR}(k, A)] \geq 1/2 + 1/\phi(k)$ for some polynomial ϕ.
We know that

$$\Pr[S_{QR}(k, A)] = \Pr[S_{QR}(k, A)|\gamma(\phi, n)]P_\gamma + \Pr[S_{QR}(k, A)|\overline{\gamma(\phi, n)}](1 - P_\gamma).$$

Furthermore, we know that $\Pr[S_{QR}(k, A)|\gamma(\phi, n)] \leq 1$, because it is a probability, and we know that $\Pr[S_{QR}(k, A)|\overline{\gamma(\phi, n)}] < 1/2 + 1/2\phi(k)$ by definition of "good." Thus, we know that

$$P_\gamma + (1/2 + 1/2\phi(k))(1 - P_\gamma) > \Pr[S_{QR}(k, A)] \geq 1/2 + 1/\phi(k)$$

and thus, we can deduce

$$\begin{aligned}
P_\gamma(1 - 1/2 - 1/2\phi(k)) + 1/2 + 1/2\phi(k) &\geq 1/2 + 1/\phi(k) \\
P_\gamma(1/2 - 1/2\phi(k)) &\geq 1/2\phi(k) \\
P_\gamma &\geq \frac{1}{2\phi(k)(1/2 - 1/2\phi(k))} \\
&= \frac{1}{\phi(k) - 1}
\end{aligned}$$

So since ϕ is a polynomial, $P_\gamma \geq \frac{1}{p(k)}$ where $p(k) = \phi(k) - 1$ is a polynomial. □

So, we have shown that if we always use steps 3 and 4 when n is good, and we always use step 2 for our output when n is not good, then we are successful with probability at least $1 - q + 1/p'(k)$. Now, I claim (without giving a proof) that the probability that n is good but we use step 2 is approximately equal to the probability that n is not good but we use steps 3 and 4, which is approximately equal to $1 - 2^{-k}$ for sufficiently large $\psi(k)$. Given this, we need to prove only the final claim.

Theorem 3 *This reduction is successful with probability at least $1 - q + 1/p''(k)$ where $1/p''(k)$ is a nonnegligible function.*

Proof. We know that

$$\begin{aligned}
P \leq\ & P_\gamma(\Pr[S_{q-GM}(k, A')|\gamma(\phi, n)](1 - 2^{-k}) + (1 - q)2^{-k}) + \\
& (1 - P_\gamma((1 - q)(1 - 2^{-k}) + \Pr[S_{q-GM}(k, A')|\overline{\gamma(\phi, n)}]2^{-k})
\end{aligned}$$

Now,

$$\begin{aligned}
P &\geq P_\gamma(1 - 2^{-k})^2 + (1 - P_\gamma)(1 - 2^{-k})(1 - q) \\
&= (1 - 2^{-k})(P_\gamma(1 - 2^{-k}) + (1 - P_\gamma)(1 - q))
\end{aligned}$$

By theorem 1, and from this last inequality, we have that

$$\begin{aligned}
P &\geq (1-2^{-k})(1-q+1/p'(k)) \\
&= 1-q+\left(\frac{1-2^{-k}}{p'(k)}-2^{-k}+q2^{-k}\right) \\
&\geq 1-q+\left(\frac{1-2^{-k}-2^{-k}p'(k)}{p'(k)}\right) \\
&= 1-q+\frac{1}{p''(k)},
\end{aligned}$$

where $p''(k)=\frac{p'(k)}{1-2^{-k}-p'(k)2^{-k}}$. Since 2^{-k} goes to zero faster than $p'(k)$ goes to infinity, we know that

$$lim_{k\to\infty}(p''(k)-p'(k))=0,$$

so we can conclude that $1/p''(k)$ is a nonnegligible function. □

The only detail left to resolve is that this relies in some sense on A' "knowing" the $\phi(k)$ such that A's advantage was $1/\phi(k)$. Truthfully, if we wanted to find out what $\phi(k)$ was, we could (to some level of accuracy), but it's much simpler to think of this setting up many reductions $A'_{\phi,\psi}$, and this proof establishing that for any A, there is a ϕ and ψ such that $A'_{\phi,\psi}$ defeats the q-GM security of the Goldwasser-Micali cryptosystem. Thus, if the Goldwasser-Micali cryptosystem is q-GM-secure, then it is GM secure.

What's special about the GM cryptosystem?

Part of the point of offering this problem followed by problem 3 was to illustrate that the GM cryptosystem has some special property, which lets us prove that q-GM security implies GM-security for this cryptosystem though we aren't able to prove this in general. These proofs are quite technical, so I thought it would be beneficial to take a high-level stab at explaining what we can do with the GM cryptosystem that we can't do with a general cryptosystem.

For the reduction in problem 2, we wanted to use the adversary repeatedly to pump up the probability so that we could be very certain of the answer, which allows us to beat probability $1-q$. In order for the probabilities to multiply over multiple trials, we needed each trial to be independent, but we couldn't actually achieve independence. We were able to use new randomness each time and a new random ciphertext each time, but we couldn't rerandomize the public key. However, we found a way out - see if we get an advantage with the given public key first. If so, use that advantage; if not, just guess.

However, the key ability we had was the ability to supply a random ciphertext each time. If r is chosen randomly, r^2c is a random encryption of the same bit that c is an encryption of, and r^2xc is a random encryption of the opposite bit that c is an encryption of. Thus, though we were giving the algorithm independent random encryptions to solve each time, we could actually use the answer.

In general, we would not necessarily have this property, and thus we might only be able to get a useful answer by asking the given adversary about the ciphertext we are given as input to the reduction. Furthermore, we can't apply the trick of seeing whether the adversary is "good" at cracking this particular ciphertext, because we can't interpret the results. If you try to apply a similar reduction to the one shown above for the general case, this is the problem you will run into.

This property that Goldwasser-Micali has is called *random self-reducibility.* It is a very useful property to be aware of and is not unique to this cryptosystem. A good exercise would be to formulate a definition for random self-reducibility of a cryptosystem, and prove that if (G, E, D) is a q-GM secure cryptosystem which is random self-reducible, then (G, E, D) is GM-secure.