CS6222 Grad Cryptography, Homework 3

Response by: Your Name, (Computing ID)

Total points: 40 awarded maximum. 50 available. Points are noted after each problem.

Instructions. For each problem, typeset your solution in the `answer` environment, and if there are sub-problems, mark them clearly. Use as much space as you require, and be sure to update your name and computing ID above, and the acknowledgements box at the end.

Policies. In short, you are encouraged to think about the problems on your own, and then discuss them and work toward solutions with your classmates. You must write and submit your own solutions. You may also read any published material that helps you come to an understanding of the problems, but you must acknowledge and/or reference any discussion or published material, with the exception of lecture notes, in-class and in-office-hours discussions, textbook sections we have covered, and basic LaTeX help or dictionary lookups. It is a violation of the honor code if any of the following occur:

- You copy text directly from any source.
- You use any material or discussion without acknowledgment or citation, excluding the above special cases.
- You are unable to explain your work orally.

See https://jackdoerner.net/teaching/2025/Fall/CS6222/#policies for more details.

Problem 1 (Don't Believe Everything You Read Online (5pts))**.** On page 64 of the Pass-shelat textbook, the authors claim that if any OWF exists, then the following function is a weak OWF:[1]

ALGORITHM 64.2: A UNIVERSAL ONE-WAY FUNCTION $f_{\text{UNIVERSAL}}(y)$

Interpret y as $\langle M, x\rangle$ where $|M| = \log(|y|)$
Run M on input x for $|y|^3$ steps
if M terminates **then**
  Output $M(x)$
else
  Output $\perp$
end if

However, there is a *critical* mistake in their version of $f_{\text{UNIVERSAL}}$.[2] It *should* say **if** M terminates **then** Output $M(x)\|M$. In other words, $f_{\text{UNIVERSAL}}$ *should* output a description of M along with $M(x)$. Demonstrate that the $f_{\text{UNIVERSAL}}$ of Pass and shelat (which does not output a description of M) is *not* weakly one-way by designing an adversary that inverts it with probability 1 for sufficiently large $n = |y|$. You may make reasonable assumptions about the encoding that $f_{\text{UNIVERSAL}}$ uses to interpret M.

[1] Note that Pass and shelat use $\langle a, b\rangle$ to denote the concatenation of a and b. In class, we usually indicate concatenation using $a\|b$, and use $\langle a, b\rangle$ for inner product.

[2] Which your instructor repeated in class, even though he had already planned this homework problem exploring it. How embarassing.

Simplification: Assuming that $f_{\text{UNIVERSAL}}$ always outputs exactly $|y|^3$ bits (which is the maximum number due to the runtime bound on M) will make your solution much simpler. You are welcome to make this assumption,[3] and you will not be penalized for doing so.

Problem 2 (Hard-Core Will Never Die but You Will (15pts total))**.** In class, we proved the Goldreich-Levin theorem, which states that for any one-way function $f : \{0,1\}^* \to \{0,1\}^*$, if we define $g : x\|r \mapsto f(x)\|r$ such that $|x| = |r|$, then the function $\mathsf{gl} : x\|r \mapsto \langle x, r\rangle \bmod 2$ is a hard-core predicate for g.[4] Notice that the Goldreich-Levin theorem *only* guarantees that gl is hard-core for g, and says nothing about the relationship between gl and f.

(a) (5pts) In class, we hand-waved the fact that if f is a one-way function, then g is also a one-way function. Write a reduction to invert f given an an adversary that can invert g, and reason about your reduction's success probability.

(b) (5pts) Suppose we define a predicate that simply outputs the i^{th} bit of its input. That is, for $1 \le i \le n$ let $\mathsf{hc}_i : x_1\| \ldots \|x_n \mapsto x_i$. Prove that if there exists some one-way function f, then there is a function g' such that no hc_i for $1 \le i \le n$ is hard-core for g'. In other words, prove that there is a OWF for which no specific input bit is hard-core.[5]

(c) (5pts) Finally, prove that for any one-way function f and any predicate hc that is hard-core for f, there exists another function g'' such that g'' is one-way, but hc is not hard-core for g''. In other words, prove that no predicate is hard-core for all one-way functions.[6]

Hint: A predicate p is certainly not hard-core for g if $g(x)$ directly leaks $p(x)$.

Problem 3 (OWF or Not? (3pts each))**.** Let $f : \{0,1\}^* \to \{0,1\}^*$ be a (strong) OWF, let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG, and let $\{F_k : \{0,1\}^{|k|} \to \{0,1\}^{|k|}\}_{k\in\{0,1\}^*}$ be a PRF family. For each of these sub-problems you must determine whether the proposed constructions of g are *necessarily* OWFs or not. Justify your answer by providing either a short proof (if g *must be* a OWF), or disproof (if it *might not be*). A disproof consists of an algorithm that inverts g with non-negligible probability over the choice of input. A disproof might depend the particular details of f, G, or F_k, in which case you should describe the f, G, or F_k on which your disproof depends, and prove that it is a OWF, PRG, or PRF, respectively.

(a) $g : x \mapsto f(x)\|f(f(x))$ [7]

(b) $g : x \mapsto f(x)\|x_1$ where x_1 is the first bit of x.

(c) $g : x \mapsto f(x)\|x_1\| \ldots \|x_{n/2}$ where $n = |x|$ and x_i is the i^{th} bit of x.

(d) $g : x \mapsto G(x)$

(e) $g : x\|y \mapsto F_x(y)$ where $|y| = |x|$

[3] Specifically, imagine a version of Pass and shelat's $f_{\text{UNIVERSAL}}$ that uses 0s to pad its output to $|y|^3$ bits

[4] Unlike Pass and shelat, we use $\langle x, r\rangle$ to denote the inner product, so if $x_1\| \ldots \|x_{|x|} = x$ and $r_1\| \ldots \|r_{|x|} = r$, then

$$\langle x, r\rangle \bmod 2 = \bigoplus_{i\in[|x|]} x_i \cdot r_i$$

[5] This means that there exists a one-way function that doesn't hide any specific bit of its input!

[6] This means that gl is the closest we can come to a *universal* HCP.

[7] Remember, we decided in class that $f(f(x))$ is *not* necessarily a OWF.

Problem 4 (Amplifying a DL Attack (5pts total))**.** Let $\mathbb{G}$ be a cyclic abelian group of prime order q,[8] with generator g. The group operation of $\mathbb{G}$ will be denoted using the multiplication symbol.[9] Suppose that there exists a PPT adversary $\mathcal{A}$ that computes *average-case* discrete logarithms in $\mathbb{G}$ with probability at least 0.01. In other words, suppose that

$$\Pr[\mathcal{A}(g^x) = x : x \leftarrow \mathbb{Z}_q] \geq 0.01.$$

Prove that if the above $\mathcal{A}$ exists, then there must also exist some PPT $\mathcal{B}$ that computes *worst-case* discrete logarithms in $\mathbb{G}$ with probability at least 0.99. That is, use $\mathcal{A}$ to construct $\mathcal{B}$ such that $\forall x \in \mathbb{Z}_q$

$$\Pr[\mathcal{B}(g^x) = x] \geq 0.99.$$

Hint: Note that $\mathcal{B}$ needs to do two different things: 1. turn a worst-case problem into the kind of average-case problem that $\mathcal{A}$ can (with probability 0.01) solve, and 2. amplify the probability that $\mathcal{A}$ succeeds. You can reason about these two things separately.

Problem 5 (From Assumption to PRG, Directly. (10pts total))**.** Let $\mathsf{GroupGen}$ be a PPT function that samples prime-order cyclic abelian groups. That is, let $(g, q) \leftarrow \mathsf{GroupGen}(1^n)$ be such that g is the *generator* of a group $\mathbb{G} = \langle g \rangle$, where $|\mathbb{G}| = q$ and q is prime. The operation of all groups produced in this way will be denoted using the multiplication symbol.[9] The *Decisional Diffie-Hellman (DDH)* assumption relative to $\mathsf{GroupGen}$ says that

$$\{(g^x, g^y, g^z) : x, y, z \leftarrow \mathbb{Z}_q, (g, q) \leftarrow \mathsf{GroupGen}(1^n)\}_{n\in\mathbb{N}}$$
$$\approx_c \{(g^x, g^y, g^{x\cdot y}) : x, y \leftarrow \mathbb{Z}_q, (g, q) \leftarrow \mathsf{GroupGen}(1^n)\}_{n\in\mathbb{N}}$$

That is, $g^{x\cdot y}$ is *indistinguishable* from g^z when x, y, z are uniform, even if the adversary is allowed to observe g^x and g^y. As a direct corollary of the DDH assumption, we can see that the function

$$\mathsf{DDHPRG}_{g,q} : (x, y) \mapsto (g^x, g^y, g^{x\cdot y})$$

is a PRG *collection*[10] from the domain $\mathbb{Z}_q^2$ to the range $\mathbb{G}^3$. Now consider a generalized form of the above function:

$$\mathsf{DDHPRG}_{g,q,\ell} : (x, y_1, \ldots, y_\ell) \mapsto (g^x, g^{y_1}, g^{x\cdot y_1}, \ldots, g^{y_\ell}, g^{x\cdot y_\ell}).$$

There are two sub-problems:

(a) (2pts) Give a formal definition for PRG collections that captures the above construction. Note that there is not a standard definition for PRG collections. I am asking you to be creative.[11] For inspiration, look at the PRG definition and the OWF collection definition.

[8] We are discussing a fixed group, but it might help you to imagine that $|q| = n$ for security parameter n.

[9] The operation denoted by $\cdot$ may or may not literally be multiplication, but regardless we define

$$g^x = \underbrace{g \cdot g \cdot g \cdot \ldots \cdot g}_{x \text{ times}}.$$

[10] PRG collections are to PRGs as OWF collections are to OWFs. Notice that q and $\mathbb{G}$ have to change as the security parameter n gets bigger!

[11] Creating definitions is an art, and as Marshall McLuhan said, *art is anything you can get away with* [MF67]. By contraposition, it's not art if you don't get away with it. Rest assured that you will be called out for writing intentionally bad definitions to make the next part of the problem easier.

(b) (8pts) Prove that if the DDH assumption is true, then $\mathsf{DDHPRG}_{g,q,\ell}$ is a PRG collection from $\mathbb{Z}_q^{\ell+1}$ to $\mathbb{G}^{2\ell+1}$.

Hint: There are two ways you could do this proof. The first way is a little bit tedious: it involves a sequence of $\ell + 1$ hybrid experiments, and a reduction that breaks the DDH assumption with advantage ε/ℓ, given a distinguisher for the PRG game that has advantage ε. The second way is short and sweet, and involves no hybrids at all: instead you can use a randomized reduction that takes (g^x, g^y, g^z) as input and performs group operations to produce an input for the PRG distinguisher that is either uniformly distributed over $\mathbb{G}^{2\ell+1}$ if z is uniformly distributed in $\mathbb{Z}_q$, or uniformly distributed over the image of $\mathsf{DDHPRG}_{g,q,\ell}$ if $z = x \cdot y$. Either way of doing the proof is acceptable, but the second way is a better exercise.

Acknowledgments

In this box, you should acknowledge your collaborators and the resources you used, if any. For example:

Problem 1: I discussed this problem with Alice and Bob. In addition, I asked Carol for help understanding Conditional Probability, but we did not discuss the problem further.

Problem 2: I asked ChatGPT "What is a turing machine?", and it gave me the following transcript: https://chatgpt.com/share/68b4dba7-e19c-8013-a137-e8db901493b7.

Problem 3: It helped me to read the proof of [Vad12, Theorem X, Page Y].

Instructor's Acknowledgments

Problems in this homework have been borrowed from or inspired by a number of sources. Citations can be provided on request, after the homework is completed.

References

[MF67] Marshall McLuhan and Quentin Fiore. *The Medium is the Massage: An Inventory of Effects*. Bantam Books, New York, 1967.

[Vad12] Salil P. Vadhan. *Pseudorandomness*. 2012. https://people.seas.harvard.edu/~salil/pseudorandomness/pseudorandomness-published-Dec12.pdf.