A Few Reductions Between Decisional Problems

CFAIL

Abstract

We state three decisional problems in prime order groups and give some reductions between them. Can you find the line that's wrong?

1 The Problems

Let G be a group of prime order p, generated by g. All lower case letters will represent values chosen uniformly and independently at random from $\mathbb{Z}_p$.

Problem 1 Given g, g^a, g^b, distinguish $T = g^{ab}$ from $T = g^r$.

Problem 2 Given g, g^{a^2}, g^b, distinguish $T = g^{a^2 b}$ from $T = g^r$.

Problem 3 Given g, g^a, g^b, g^c, g^{ac}, distinguish $T = g^{ab}$ from $T = g^r$.

2 The Reductions

Theorem 1. *Given a PPT algorithm $\mathcal{A}'$ that achieves non-negligible advantage in Problem 1, we can build a PPT algorithm $\mathcal{A}$ that achieves non-negligible advantage in Problem 2.*

Proof. We define $\mathcal{A}$ as follows. $\mathcal{A}$ receives input g, g^{a^2}, g^b, and T.
It samples c itself, uniformly at random from $\mathbb{Z}_p$. It implicitly sets $a' = a^2 c$.
It can then efficiently compute $g^{a'} = (g^{a^2})^c$ and T^c.
It sends g, $g^{a'}$, g^b, T^c to $\mathcal{A}'$ and copies its answer.
The advantage of $\mathcal{A}$ is negligibly close to the advantage of $\mathcal{A}$.

$\square$

Theorem 2. *Given a PPT algorithm $\mathcal{A}'$ that achieves non-negligible advantage in Problem 2, we can build a PPT algorithm $\mathcal{A}$ that achieves non-negligible advantage in Problem 1.*

Proof. We define $\mathcal{A}$ as follows. $\mathcal{A}$ receives input g, g^a, g^b, and T.
It sends these inputs to $\mathcal{A}'$ and copies its answer.
When a is a square, this matches the input distribution of Problem 2.
The value a is square in $\mathbb{Z}_p$ with probability at least $\frac{1}{2}$, as half of the non-zero elements of $\mathbb{Z}_p$ are squares.
The advantage of $\mathcal{A}$ is thus at least $\frac{1}{2}$ the advantage of $\mathcal{A}'$, and hence non-negligible. $\square$

Theorem 3. *Given a PPT algorithm $\mathcal{A}'$ that achieves non-negligible advantage in Problem 3, we can build a PPT algorithm $\mathcal{A}$ that achieves non-negligible advantage in Problem 1.*

Proof. We define $\mathcal{A}$ as follows. $\mathcal{A}$ receives input g, g^a, g^b, and T.
It samples c itself, uniformly at random from $\mathbb{Z}_p$.
It can then efficiently compute g^c and $g^{ac} = (g^a)^c$.
It sends g, g^a, g^b, g^c, g^{ac}, T to $\mathcal{A}'$ and copies its answer.
The advantage of $\mathcal{A}$ is identical to the advantage of $\mathcal{A}'$.

$\square$

actually $2 \cdot$ adv. of $A' - \frac{1}{2}$, could be negl.