On the Bit Security of Cryptographic Primitives

CS6160: Cryptology Paper Presentation

CS18BTECH11001 - A. Sai Mahesh

Indian Institute of Technology, Hyderabad

November 22, 2021

This document is generated by LaTeX

1 Introduction

Let's start with discussing the common term of bit security used by the cryptographer and point out the problems that cannot be solved using the current definition. Let's then proceed ahead to newer definition of bit security and show how the above problem can be solved using our new definition. We then move on defining our notion for general type of cryptographic primitives and then show that this notion can be applied for both search and decision problem. Finally, we look at more results that can be deduced from our newer notation and how can it be extended further.

2 Common Definition of Bit Security

The cryptographer's commonly use the word bit security to denote the exponential relation of resources required by the adversary to break the cryptographic primitive. They commonly agreed to the following definition:
Definition: A cryptographic primitive is said to be n-bit secure, if any Adversary with incurring cost T and success probability ϵ must satisfy

$$\frac{T}{\epsilon} > 2^n$$

3 Paradoxical Situations in the definition

Although the common definition described above provide the asymptotic(qualitative) and concrete(quantitative) description, It cannot able to handle the case of non-uniform setting where the adversary can receive an additional advice.
Example: A Pseudo Random Generator(PRG) with seed length n cannot provide more than n/2 bits of security.

4 Newer Definition of Bit Security

The bit security is determined using the security games where the adversary has to guess the n-bit string chosen by the challenger. Based on these games the primitives are classified as search and decision where search indicates the recovery of key over a n-bit key space and decision indicates the guessing whether the bit is 0 or 1(i.e., n = 1).

We now introduce an extra term of "don't know" symbol $\perp$ for the adversary output which expresses the clear understanding of adversary accepting the defeat rather than outputting random guess. Then we introduce some terms that can be used in prove the further results - $\boldsymbol{R(X,A)}$, $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\epsilon}$, $\boldsymbol{\delta}$. Refer to the presentation for definitions of these terms.

5 Solving Paradoxical Situation

We can now represent the advantage of adversary over non-uniform setting with the term "adversary advantage" and can be defined for search primitive as the probability of finding the success information given by $\boldsymbol{\epsilon = \alpha\beta}$ where as for decision primitive as the probability of correct output over the probability of random guess and given by $\boldsymbol{\alpha\delta^2, \delta = 2\beta - 1}$.

Now for the above discussed example of PRG by simply considering the adversarial advantage as $\delta = 2^{-n/2}$ we can say that it achieves $\log_2\left(\frac{T}{\delta^2}\right) = n$-bit security even in constant time and thus resolving the above paradoxical situation.

6 Generalizing adversary advantage

The general form of adversary advantage can be given by:

$$adv = \alpha\left(1 - \frac{(1-\beta)\,log(2^n - 1) + H\left(B_\beta\right)}{n}\right)$$

We can deduce the equations for both search and decision primitives from the above definition as shown below and thus making our new definition to work much concrete.

Search Primitive

for large n:

$$2^n - 1 \sim 2^n$$

$$adv = \alpha\left(1 - \frac{(1-\beta)\,log(2^n) + H\left(B_\beta\right)}{n}\right)$$

$$adv = \alpha\left(1 - \frac{n\,(1-\beta) + constant}{n}\right)$$

$$adv = \alpha\left(1 - (1-\beta) + \frac{constant}{n}\right)$$

$$adv \sim \alpha\beta$$

Decision Primitive

for n = 1:

$$adv = \alpha\left(1 - \frac{0 + H\left(B_\beta\right)}{1}\right)$$

$$adv = \alpha\left(1 - H\left(B_\beta\right)\right)$$

$$adv = \alpha\left(1 + \beta\log\beta + (1-\beta)\log\left(1-\beta\right)\right)$$

$$adv = \alpha\left(\frac{\delta^2}{2ln2} + O\left(\delta^4\right)\right)$$

$$adv \sim \alpha\delta^2$$

7 Security Deductions

By using our new definition we can construct one primitive from other such as decision from search problem, search from decision primitive or decision from other decision problem and we can also prove some more results and can be able to provide tighter bounds for some problems. One such result is proving that the Pseudo Random Generator(PRG) is a One way function(OWF) of same security level and we can show that OWF implies that Goldreich-Levin hardcore bit is a PRG of same security level. Further this definition is used to prove the that Indistinguishably chosen ciper text attack(IND-CCA) secure encryption can provide message hiding property. Finally, we are able to provide a tight reduction of approximating a distribution with floating point numbers with half the bit security($\frac{n}{2}$) as mantissa with a relative error of $2^{-n/2}$ can preserve all the n-bit security.

8 Conclusion

Our Work can be further extended to clarify the bit security of lattice-based cryptographic primitives(refer to this article). The ability of outputting the don't know symbol and accepting the defeat by the adversary is the key step involved and which lead to define various definition that can be used under non-uniform setting where the adversary can receive an additional advice and our definition depending upon the depth of the advice(adversary advantage).