On the Bit Security of Cryptographic Primitives

CS6160: Cryptology Paper Presentation

CS18BTECH11001 - A. Sai Mahesh

Indian Institute of Technology, Hyderabad

November 25, 2021

Outline

- Bit Security of Cryptographic Primitives
- Security games of Cryptographic Primitives
- Paradoxical Situations in current definition
- New Notation of Bit Security
- The Adversary Advantage
- Security Reductions
- Further Work
- Conclusion

Bit Security of Cryptographic Primitives

The level of security offered by a cryptographic Primitive P
= number of bits of security(n) provided by the primitive
= running a brute force attack on the n-bit key space.

Definition 1: n bits security of cryptographic primitive

Any attack that successfully break an n bits secure cryptographic primitive P with a cost T and success probability ϵ must have

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

Note: Definition is introduced from [1]

Bit Security of Cryptographic Primitives

Definition 1 satisfies the both approaches of bit security.

1. Asymptotic Approach: Identify feasible adversaries with polynomial time computation and provide qualitative classification of cryptographic functions

Figure 1: Bit security fits between both approaches. `Refer here.`

2. Concrete Approach: Express adversary's cost using different components like time complexity, space complexity etc and provide quantitative approach in the form of a single number - bit security.

Security games of Cryptographic Primitives

The security of a cryptographic primitive is defined using the security games. It is a game in which an adversary has to guess an n-bit secret string. The primitives are classified into two type based on the type of games that define their security.

- Search Primitive:
  - Recover secret from large search space
  - Eg: Key Recovery Attack
- Decision Primitive:
  - Decide if a secret bit is 0 or 1
  - Eg: Indistinguishability games

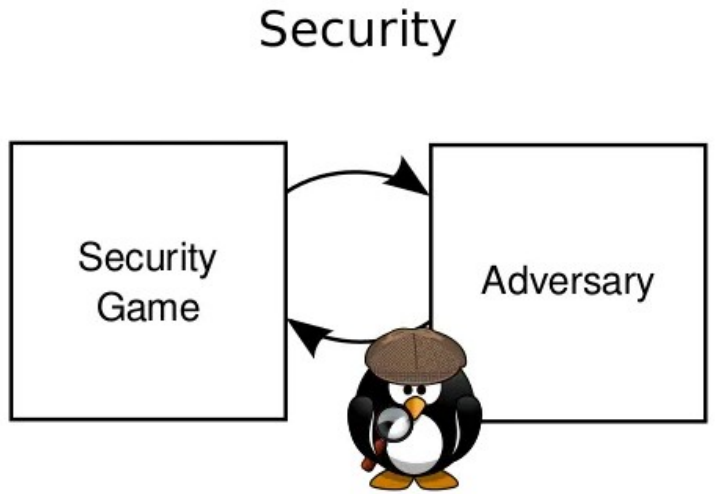

Figure 2: Security Game of adversary.

Refer here.

Paradoxical Situations in current definition

If there is a non-uniform setting where an adversary may receive an additional advice, considering only the adversary's resources is a poor measure of the cost of an attack and insufficient to address this issue.

Example: A PRG function $f : \{0,1\}^n \rightarrow \{0,1\}^m$, where $m > n$ with seed length n cannot provide more than n/2 bits of security according to Definition 1. This can be explained from Lemma 1.

Key size		Security level (bits)
RSA/DSA	ECC	
1024	160	80
2048	224	112
3072	256	128
7680	384	192
15360	**521**	256

Figure 3: Security level of algorithms with respective key size. Refer [2]

Paradoxical Situations in current definition

To understand these paradoxical situations better let us introduce the term distinguishing advantage caused from non-uniform attacks. The advantage for different type of primitives as follows:

- search Primitive: Probability of finding secret information.
- decision Primitive: Probability that the output of adversary is correct over the trivial probability that of $\frac{1}{2}$ of a random guess.

Lemma 1: Distinguishing advantage of PRG

The non-uniform attacks on a PRG with seed length n achieve the distinguishing advantage of $2^{-\frac{n}{2}}$

Note: The above lemma is summarised from [1]

New Notation of Bit Security

We now define our new definition to the bit security.

Definition 2: New notation of bit security

During the game of adversary guessing the n-bit string we add a distinguishing feature of allowing adversary to output a special "don't know" symbol $\perp$ rather than a random guess.

Let us introduce the following terms:
α - Probability that adversary output something other than $\perp$
β - conditional Probability that the output correctly identifies the secret.
ϵ - Success Probability.
δ - Conditional Distinguishing advantage

The Adversary Advantage

The amount of information that the adversary is able to know about the secret is knows as Adversary Advantage. The Adversary Advantage of different primitives is given below

Cryptographic Primitive	Adversarial Advantage	Bit Security
Search Primitive	$\epsilon = \alpha\beta$	$\log_2\left(\frac{T}{\epsilon}\right)$
Decision Primitive	δ^2, $\delta = 2\beta - 1$	$\log_2\left(\frac{T}{\alpha\delta^2}\right)$

Table 1: Adversary Advantage of Cryptographic Primitives

Using our definition and by considering the PRG with an adversary advantage of $\delta = 2^{-\frac{n}{2}}$ in non-uniform attacks, 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.

The Adversary Advantage

Result: Adversary Advantage for a general primitive

The advantage of adversary outputting a value A played over a challenger with a chosen secret $X \in \{0,1\}^n$ can be given by

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

where $R(X, A) \rightarrow$ Relation between adversary output and secret key

$\alpha = P[A \neq \perp]$

$\beta = P[R(X, A) | a \neq \perp]$

H is the Shannon Entropy

B_β is Bernoulli Distribution with parameter β

Note: The relation R can be considered as Identity Relation R(x,x). Refer [1]

Security Reductions

Our newer definitions can be used to several reductions. We can

1. Construct Search primitive from Decision Primitive
2. Construct Decision Primitive from Search Primitive
3. Construct Decision Primitive from other Decision Primitive
4. Relation between bit security of OWF and PRG

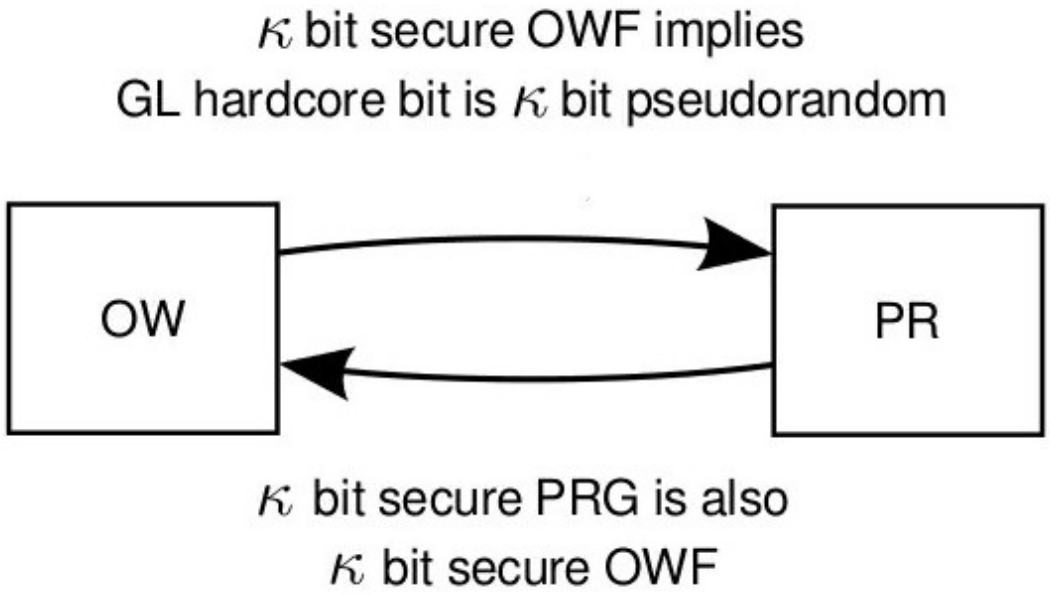

Figure 4: Relation between OWF and PRG. `Refer here.`

Security Reductions

5. Indistinguishability under chosen cipertext attack(IND-CCA) implies OWF
6. If a scheme with message space larger than 2^{κ} is κ-bit IND-CCA secure, it is κ-bit message hiding.
7. Prove that approximating a distribution with a relative error of $2^{-\kappa/2}$ using floating point numbers with $\kappa/2$ mantissa can preserve almost all κ bits of security.

Further Work

We can extend our definition in the below aspects.

1. Our definition can be used to improve the security proofs for the lattice based Cryptography Primitives. Refer to [3] for further reference.
2. Our definition can be used to provide Sharper Bounds in Lattice-Based Cryptography. Refer to [4] for further reference.

Conclusion

- Introducing of the "don't know" symbol $\perp$ with the adversary admitting the failure became more informative rather than a random guess and resulted in much tighter reductions.
- Our definitions has successfully explained the paradoxical situations by introducing the term "adversary advantage" which cannot be explained by the common definition used.
- Our further security reductions has shown numerous results in the advancement of cryptography.

References

- Daniele Micciancio, Michael Walter. On the Bit Security of Cryptographic Primitives, May 2019.
- Chandel, Sonali Cao, Wenxuan Sun, Zijing Yang, Jiayi Zhang, Bailu Ni, Tian-Yi. (2020). A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption. 10.1007/978-3-030-12385-7_67.
- S. Bai, A. Langlois, T. Lepoint, D. Stehl´e, and R. Steinfeld. Improved security proofs in lattice-based cryptography: Using the R´enyi divergence rather than the statistical distance, Dec 2015.
- T. Prest. Sharper bounds in lattice-based cryptography using the R´enyi divergence, Dec 2017