Foundations of Cryptography

Notes of lecture No. 7 (given on Apr. 16th)

Notes taken by Michal Seidmann and Nir Dvir

Summary

In this lecture we deal with the two definitions of security of encryption schemes that were presented in the last lecture - semantic security and security in the sense of indistinguishability - and with the relation between them. We claim and prove the theorem stated at the end of the last lecture : Security in the sense of indistinguishability implies semantic security. We introduce the notion of *decomposability,* and then claim and prove that under the condition of decomposability, semantic security implies security in the sense of indistinguishability .

1. Security in the sense of indistinguishability of encryptions implies semantic security.

Theorem 1: If an encryption scheme (G,E,D) is secure in the sense of indistinguishability of encryptions, then it is semantically secure.

As we have already mentioned, we claim (and prove later) that the converse implication also holds (under some additional condition). Nevertheless, the above is the interesting implication, since the existence of encryption schemes which are secure in the sense of indistinguishability will be proved, and this fact, together with the theorem, implies the existence of semantically secure encryption schemes.

We will give first a short sketch of the proof, and then we will formally complete the missing details .
Let $\{X_n^{(1)}\}$ be a sequence of [polynomial] random variables, let h be a [polynomially computable] function, let f be a function and let A be a polynomial algorithm (trying to guess $f(X_n)$ from $h(X_n)$ and $E_{G(1^n)}(X_n)$). Define $\{X_n^{(2)}\}$, a sequence of [polynomial] random variables independent of $\{X_n^{(1)}\}$, but with the same distribution as $\{X_n^{(1)}\}$. Using the hypothesis that encryptions by (G,E,D) are indistinguishable, we will show that

$$\text{Prob}\left[A(E_{G(1^n)}(X_n^{(1)}),\ h(X_n^{(1)}),\ 1^n) = f(X_n^{(1)})\right] \approx \text{Prob}\left[A(E_{G(1^n)}(X_n^{(2)}),\ h(X_n^{(1)}),\ 1^n) = f(X_n^{(1)})\right] \qquad (1)$$

This approximation seems reasonable - if $E_{G(1^n)}(X_n^{(1)})$ and $E_{G(1^n)}(X_n^{(2)})$ cannot be distinguished, then A should ‘behave’ similarly given each one of them as A’s input, because if there is a significant difference in A’s ‘behaviour’ then this difference can be used to construct a distinguishing algorithm. Nevertheless, this must be proved precisely, since it is not so obvious (especialy in the uniform case) how "different behaviour" can be translated into one bit with different probability.

Assuming we have shown the above (1), we can construct a polynomial algorithm A' , that given $h(X_n^{(1)})$ as its input , samples $X_n^{(2)}$ (if A' is uniform) or uses "its in-built" $X_n^{(2)}$ (if A' is non-uniform), and simulates A . i.e.

$$A'(h(X_n^{(1)}),\ 1^n) = A(E_{G(1^n)}(X_n^{(2)}),\ h(X_n^{(1)}),\ 1^n)$$

Using (1) we get:

$$\mathrm{Prob}\left[A(E_{G(1^n)}(X_n^{(1)}),\ h(X_n^{(1)}),\ 1^n) = f(X_n^{(1)})\right] \approx \mathrm{Prob}\left[A'(h(X_n^{(1)}),\ 1^n) = f(X_n^{(1)})\right]$$

which implies that (G,E,D) is semantically secure.
In order to complete the proof of Theorem 1, the next lemma (which states formally the approximation (1) above) will be proved.

Lemma: Let (G,E,D) be an encryption scheme which is secure in the sense of indistinguishability of encryptions, let $\{X_n^{(1)}\}$ be a sequence of [polynomial] random variables, let h be a [polynomially computable] function , let f be a function and let A be a probabilistic polynomial-time algorithm.
Given $\{X_n^{(2)}\}$, a sequence of [polynomial] random variables independent of $\{X_n^{(1)}\}$, but with the same distribution as $\{X_n^{(1)}\}$, the following inequality holds :

$$\mathrm{Prob}\left[A(E_{G(1^n)}(X_n^{(1)}),\ h(X_n^{(1)}),\ 1^n) = f(X_n^{(1)})\right] - \mathrm{Prob}\left[A(E_{G(1^n)}(X_n^{(2)}),\ h(X_n^{(1)}),\ 1^n) = f(X_n^{(1)})\right] < \frac{1}{n^c}$$

As usual, there are two formulations for this Lemma: for the uniform and the non-uniform case, obtained by including or excluding the brackets respectively.
Note: Recall that ‘ $X_n^{(2)}$ *is independent of* $X_n^{(1)}$ ’ means:

$$\forall \alpha,\beta \in \{0,1\}^n \quad \mathrm{Prob}\left[(X_n^{(1)} = \alpha) \wedge (X_n^{(2)} = \beta)\right] = \mathrm{Prob}\,(X_n^{(1)} = \alpha) \cdot \mathrm{Prob}\,(X_n^{(2)} = \beta)$$

and ‘ $X_n^{(2)}$ *has the same distribution like* $X_n^{(1)}$ ’ means :

$$\forall \alpha \in \{0,1\}^n , \quad \mathrm{Prob}\,(X_n^{(1)} = \alpha) = \mathrm{Prob}\,(X_n^{(2)} = \alpha)$$

We prove the Lemma for both uniform and non-uniform cases. As usual, the proof for the non-uniform case is easier because it is possible to incorporate the necessary components instead of constructing them. In both cases the proof explains the total lack of restrictions on the function f .

Proof of the Lemma (Non-uniform case):

It is sufficient to prove that

$$\forall c > 0 \;\; \exists N, \;\; \forall n > N, \; \forall\, \alpha,\beta \in \{0,1\}^n$$

$$\text{Prob}\left[A\,(E_{G(1^n)}(\alpha),\, h(\alpha),\, 1^n) = f(\alpha)\right] - \text{Prob}\left[A\,(E_{G(1^n)}(\beta),\, h(\alpha),\, 1^n) = f(\alpha)\right] < \frac{1}{n^c} \qquad (2)$$

We will denote :

$$p_n \triangleq \text{Prob}\left[A\,(E_{G(1^n)}(\alpha),\, h(\alpha),\, 1^n) = f(\alpha)\right]$$

$$q_n \triangleq \text{Prob}\left[A\,(E_{G(1^n)}(\beta),\, h(\alpha),\, 1^n) = f(\alpha)\right]$$

Assume by contradiction that the lemma does not hold. Then :

$$\exists c > 0 \;\; \forall N \;\; \exists n > N, \; \exists\, \alpha_n,\beta_n \in \{0,1\}^n \quad \text{such that} \quad p_n - q_n \geq \frac{1}{n^c}$$

We will show that this implies the existence of a polynomial distinguishing algorithm A', for which $\exists c > 0 \;\; \forall N \; \exists n > N, \; \exists\, \alpha_n,\beta_n \in \{0,1\}^n$ (which will be the same α_n , β_n that were mentioned in the contradiction assumption), such that

$$\text{Prob}\left[A'(\alpha_n \circ \beta_n,\, E_{G(1^n)}(\alpha_n)) = 1\right] - \text{Prob}\left[A'(\alpha_n \circ \beta_n,\, E_{G(1^n)}(\beta_n)) = 1\right] \geq \frac{1}{n^c}$$

in contradiction with the scheme being secure in the sense of indistinguishability .

The distinguishing algorithm A' :

This algorithm is actually an infinite sequence of (non-uniform) circuits $\{A_n'\}$. For each length n, the circuit A_n' includes in its description the strings $h(\alpha_n)$ and $f(\alpha_n)$ (thus, the non-uniformity is used quite strongly since f is not necessarily computable). Given an input $\alpha_n \circ \beta_n$, $E_{G(1^n)}(\gamma)$ (for $\gamma \in \{\alpha_n , \beta_n\}$), algorithm A_n' simulates A on the input: $E_{G(1^n)}(\gamma),\; h(\alpha_n),\; 1^n$.
If $A\,(E_{G(1^n)}(\gamma),\, h(\alpha_n),\, 1^n) = f(\alpha_n)$, then A_n' outputs 1 . Otherwise, A_n' outputs 0 .

$$\text{Prob}\left[A_n'(\alpha_n \circ \beta_n,\, E_{G(1^n)}(\alpha_n)) = 1\right] = \text{Prob}\left[A\,(E_{G(1^n)}(\alpha_n),\, h(\alpha_n),\, 1^n) = f(\alpha_n)\right] = p_n$$

$$\text{Prob}\left[A_n'(\alpha_n \circ \beta_n,\, E_{G(1^n)}(\beta_n)) = 1\right] = \text{Prob}\left[A\,(E_{G(1^n)}(\beta_n),\, h(\alpha_n),\, 1^n) = f(\alpha_n)\right] = q_n$$

Therefore,

$$\text{Prob}\left[A'(\alpha_n \circ \beta_n,\, E_{G(1^n)}(\alpha_n)) = 1\right] - \text{Prob}\left[A'(\alpha_n \circ \beta_n,\, E_{G(1^n)}(\beta_n)) = 1\right] = p_n - q_n \geq \frac{1}{n^c} \quad \blacksquare$$

Proof of the Lemma (Uniform case):

The general idea of the proof is the same. We assume by contradiction that the Lemma does not hold, and present an algorithm that contradicts the security in the sense of indistinguishability of encryptions.
This time we will not be able to prove that for **all** (α, β) inequality (2) holds. We will prove instead, that it is infeasible to find a pair (α, β) that violates inequality (2), and the Lemma will follow.
Denote $X_n = X_n^{(1)} \circ X_n^{(2)}$ (recall that $X_n^{(2)}$ is the random variable which is independent of $X_n^{(1)}$ but with the same distribution). We define the following set (of "distinguishable" pairs α, β) :

$$B_n^c \triangleq \left\{ (\alpha,\beta) : \alpha\circ\beta \in \{0,1\}^{2n} ,\ \mathrm{Prob}\left[A\,(E_{G(1^n)}(\alpha),\ h(\alpha),\ 1^n) = f(\alpha)\right] - \right.$$
$$\left. - \mathrm{Prob}\left[A\,(E_{G(1^n)}(\beta),\ h(\alpha),\ 1^n) = f(\alpha)\right] > \frac{1}{n^c} \right\}$$

Claim: $\forall c > 0\ \exists N\ \forall n > N,\ \mathrm{Prob}\,(X_n \in B_n^c) < \frac{1}{n^c}$

Proof: We will introduce another set D_n^c :

$$D_n^c \triangleq \left\{ (\alpha,\beta) : \alpha\circ\beta \in \{0,1\}^{2n} \wedge \exists v\ \ s.t.\ \ \mathrm{Prob}\left[A\,(E_{G(1^n)}(\alpha),\ h(\alpha),\ 1^n) = v\right] - \right.$$
$$\left. - \mathrm{Prob}\left[A\,(E_{G(1^n)}(\beta),\ h(\alpha),\ 1^n) = v\right] > \frac{1}{n^c} \right\}$$

Obviously, $B_n^c \subseteq D_n^c$, and thus it is sufficient to prove that:

$$\forall c > 0\ \ \exists N,\ \ \forall n > N :\ \mathrm{Prob}\,(X_n \in D_n^c) < \frac{1}{n^c}$$

(note that the function f plays no role in the definition of the set D_n^c which explains why there are no restrictions on f.)

Assume by contradiction that

$$\exists c_0 > 0\ \ \forall N,\ \exists n > N,\ \mathrm{Prob}\,(X_n \in D_n^{c_0}) \geq \frac{1}{n^{c_0}}$$

We will show that this implies the existence of two polynomial algorithms, F and A'', such that

$$\mathrm{Prob}\left[F(1^n) = \alpha\circ\beta :\ \left|\mathrm{Prob}\left[A''(\alpha\circ\beta,\ E_{G(1^n)}(\alpha)) = 1\right] - \mathrm{Prob}\left[A''(\alpha\circ\beta,\ E_{G(1^n)}(\beta)) = 1\right]\right| \geq \frac{1}{n^{c_0}}\right] \geq \frac{1}{n^{c_0}} \qquad (3)$$

in contradiction with the scheme being secure in the sense of indistinguishability (according to the alternative formalization of security in the sense of indistinguishability).

F is a polynomial sampling algorithm for X_n (recall that $X_n = X_n^{(1)} \circ X_n^{(2)}$). Such an algorithm exists since X_n is a polynomial random variable (as $X_n^{(1)}$, $X_n^{(2)}$ are).

The algorithm A'' **:**

The general idea : for $(\alpha,\beta) \in D_n^{c_0}$ the algorithm tries to find a value v_0 such that

$$\text{Prob}\left[A\,(E_{G(1^n)}(\alpha),\ h(\alpha),\ 1^n) = v_0\right] - \text{Prob}\left[A\,(E_{G(1^n)}(\beta),\ h(\alpha),\ 1^n) = v_0\right] > \frac{1}{n^{c_0}} \qquad (4)$$

In order to 'find' such value v_0 the algorithm estimates the probability of every v to be a result of $A\,(E_{G(1^n)}(\alpha),\ h(\alpha), 1^n)$ or $A\,(E_{G(1^n)}(\beta), h(\alpha), 1^n)$, by computing these values sufficiently many times.
The value v that gives the maximal difference for its relative frequency as an output of $A\,(E_{G(1^n)}(\alpha), h(\alpha), 1^n)$ and its relative frequency as an output of $A\,(E_{G(1^n)}(\beta), h(\alpha), 1^n)$, will be chosen as v_0 . We will prove later that for v_0 inequality (4) holds (up to a constant), with a probability close to 1. Thus, A'' can now use this value to distinguish between the encryptions (in the way $f\,(\alpha_n)$ was used in the non-uniform algorithm).

Input : $\alpha \circ \beta$, t (t is from the $E_{G(1^n)}(\alpha)$ sample or from the $E_{G(1^n)}(\beta)$ sample)

Step I : A'' computes $E_{G(1^n)}(\alpha)$ and $E_{G(1^n)}(\beta)$, for $N \triangleq n^{2 \cdot c_0 + 1}$ times (independently), and each time computes $A\,(E_{G(1^n)}(\alpha), h(\alpha), 1^n)$ and $A\,(E_{G(1^n)}(\beta),\ h(\alpha),\ 1^n)$ (recall that the function h is polynomially computable, and thus $h(\alpha)$ can be computed).

For each value v, obtained as an output of these computations, the difference of its relative frequency as an output of $A\,(E_{G(1^n)}(\alpha),\ h(\alpha),\ 1^n)$ and its relative frequency as an output of $A\,(E_{G(1^n)}(\beta),\ h(\alpha),\ 1^n)$ is calculated. (These relative frequencies estimate Prob $\left[A\,(E_{G(1^n)}(\alpha),\ h(\alpha),\ 1^n) = v\right]$ and Prob $\left[A\,(E_{G(1^n)}(\beta),\ h(\alpha),\ 1^n) = v\right]$).

Let v_0 be a value that gives the maximal difference (if there are several such values, one of them is chosen arbitrarily). Note that v_0 is a random variable defined over the probability space of runs of algorithm A on inputs of the form $(E_{G(1^n)}(\gamma),\ h(\alpha),\ 1^n)$.

Step II : A'' computes $v = A\,(t,\ h(\alpha),\ 1^n)$

If $v = v_0$ then A'' outputs 1 .

Otherwise: A'' outputs 0 .

End of the algorithm.

Assume $(\alpha\ ,\ \beta) \in D_n^{c_0}$. We will prove that :

$$\text{Prob}\left[A''(\alpha \circ \beta\ ,\ E_{G(1^n)}(\alpha)) = 1\right] - \text{Prob}\left[A''(\alpha \circ \beta\ ,\ E_{G(1^n)}(\beta)) = 1\right] \geq \frac{1}{8 \cdot n^{c_0}} \qquad (5)$$

Since the proof is quite long and technical, the exact details can be found in appendix A. We will give here only the intuition.

Since the sampling is large enough, the relative frequencies give quite an accurate estimation of the probabilities $\text{Prob}\left[A(E_{G(1^n)}(\alpha),\, h(\alpha),\, 1^n) = v\right]$ and $\text{Prob}\left[A(E_{G(1^n)}(\beta),\, h(\alpha),\, 1^n) = v\right]$ (the deviation can be bounded by $\dfrac{1}{4 \cdot n^{c_0}}$ with high probability). By the hypothesis $(\alpha,\beta) \in D_n^{c_0}$ implying that there exists v such that

$$\text{Prob}\left[A(E_{G(1^n)}(\alpha),\, h(\alpha),\, 1^n) = v\right] - \text{Prob}\left[A(E_{G(1^n)}(\beta),\, h(\alpha),\, 1^n) = v\right] \geq \frac{1}{n^{c_0}}$$

and using the definition of the random variable v_0, it follows that

$$\text{Prob}\left[A(E_{G(1^n)}(\alpha),\, h(\alpha),\, 1^n) = v_0\right] - \text{Prob}\left[A(E_{G(1^n)}(\beta),\, h(\alpha),\, 1^n) = v_0\right] \geq \frac{1}{4 \cdot n^{c_0}}$$

with probability close to 1.

Thus, we have found a value v_0 such that there is a significant difference between $\text{Prob}\left[A(E_{G(1^n)}(\alpha),\, h(\alpha),\, 1^n) = v_0\right]$ and $\text{Prob}\left[A(E_{G(1^n)}(\beta),\, h(\alpha),\, 1^n) = v_0\right]$, and therefore, if A'' outputs 1 iff $A(t,\, h(\alpha),\, 1^n) = v_0$ it follows that there is a significant difference between $\text{Prob}\left[A''(\alpha \circ \beta\,,\, E_{G(1^n)}(\alpha)) = 1\right]$ and $\text{Prob}\left[A''(\alpha \circ \beta\,,\, E_{G(1^n)}(\beta)) = 1\right]$.

We conclude that inequality (5) holds, for $(\alpha,\beta) \in D_n^{c_0}$ and since we assumed that the probability of sampling a pair in $D_n^{c_0}$ is greater than $\dfrac{1}{n^{c_0}}$, it follows that F finds pairs that satisfy inequality (5) with a probability greater than $\dfrac{1}{n^{c_0}}$.

Inequality (3) follows, in contradiction with the scheme being secure in the sense of indistinguishability. Therefore the contradiction hypothesis was false. Namely:

$$\forall c > 0\ \exists N\ \forall n > N\quad \text{Prob}\,(X_n \in D_n^c) < \frac{1}{n^c}$$

and this implies that

$$\forall c > 0\ \exists N\ \forall n > N\quad \text{Prob}\,(X_n \in B_n^c) < \frac{1}{n^c} \qquad \Box \quad \text{(of the claim)}$$

Using the above claim, we can now complete the Lemma's proof.

$$\text{Prob}\left[A\,(E_{G(1^n)}(X_n^{(1)}),\, h(X_n^{(1)})) = f\,(X_n^{(1)})\right] - \text{Prob}\left[A\,(E_{G(1^n)}(X_n^{(2)}),\, h(X_n^{(1)})) = f\,(X_n^{(1)})\right] =$$

$$= \sum_{(\alpha,\beta) \in B_n^c} \text{Prob}\,(X_n = \alpha \circ \beta) \cdot \Big[\text{Prob}\left[A\,(E_{G(1^n)}(\alpha),\, h(\alpha),\, 1^n) = f\,(\alpha)\right] -$$

$$- \text{Prob}\left[A\,(E_{G(1^n)}(\beta),\, h(\alpha),\, 1^n) = f\,(\alpha)\right]\Big] +$$

$$+ \sum_{(\alpha,\beta) \notin B_n^c} \text{Prob}\,(X_n = \alpha \circ \beta) \cdot \Big[\text{Prob}\,\big(A\,(E_{G(1^n)}(\alpha),\, h(\alpha),\, 1^n) = f(\alpha)\big) -$$

$$- \text{Prob}\,\big(A\,(E_{G(1^n)}(\beta),\, h(\alpha),\, 1^n) = f(\alpha)\big) \Big] \leq$$

$$\leq \sum_{(\alpha,\beta) \in B_n^c} \text{Prob}\,(X_n = \alpha \circ \beta) + \sum_{(\alpha,\beta) \notin B_n^c} \text{Prob}\,(X_n = \alpha \circ \beta) \cdot \frac{1}{n^c} =$$

$$= \text{Prob}\,(X_n \in B_n^c) + \frac{1}{n^c} \cdot \text{Prob}\,(X_n \notin B_n^c) \leq$$

$$\leq \frac{1}{n^c} + \frac{1}{n^c} \cdot 1 \leq \frac{2}{n^c}$$

Therefore:

$$\forall c > 0\ \exists N',\quad \forall n > N'$$

$$\text{Prob}\,\big(A\,(E_{G(1^n)}(X_n^{(1)}),\, h(X_n^{(1)}),\, 1^n) = f(X_n^{(1)})\big) - \text{Prob}\,\big(A\,(E_{G(1^n)}(X_n^{(2)}),\, h(X_n^{(1)}),\, 1^n) = f(X_n^{(1)})\big) < \frac{1}{n^c}$$

The Lemma is thus proved, and Theorem 1 follows directly, as described in the proof sketch. ■

2. Semantic security implies security in the sense of indistinguishability.

For the sake of elegancy (...) we will prove that the converse implication (semantic security implies security in the sense of indistinguishability) also holds. But, as was noted before, another condition must be assumed.

Definition: An encryption scheme (G,E,D) is said to be *decomposable* iff given $E_{G(1^n)}(\gamma)$ such that $\gamma = \alpha \circ \beta$, $E_{G(1^n)}(\beta)$ can be computed (β is any suffix of γ).

Theorem 2: If an encryption scheme (G,E,D) is decomposable and semantically secure, then it is also secure in the sense of indistinguishability .

The condition of decomposability will be needed only in the uniform version of the theorem, and thus, it can be omitted in the non-uniform one. Therefore - in the non-uniform case, both definitions of security are equivalent. (Actually, even in the uniform case, this condition is too strong, since we will not use the ability to compute $E_{G(1^n)}(\beta)$ for any β, a suffix of γ, but only for β s.t. $|\beta| = \frac{1}{3} \cdot |\gamma|$).

Again, we prove the theorem in both uniform and non-uniform cases.

Proof of Theorem 2 (non-uniform case):

Assume by contradiction that the encryption scheme is not secure in the sense of indistinguishability. In the non-uniform case this implies the existence of a constant $c_1 > 0$ such that
$\forall N, \exists n > N, \quad \exists \alpha_n, \beta_n \in \{0,1\}^n$:

$$\text{Prob}\left[A(\alpha_n \circ \beta_n, E_{G(1^n)}(\alpha_n)) = 1\right] - \text{Prob}\left[A(\alpha_n \circ \beta_n, E_{G(1^n)}(\beta_n)) = 1\right] \geq \frac{1}{n^{c_1}}$$

We will show that this contradicts the assumption that the scheme is semantically secure, i.e. it implies the existence of a sequence of random variables $\{Z_n\}$, functions $h(Z_n)$, and $f(Z_n)$, and a polynomial algorithm A' such that for every polynomial algorithm A'' there exists a constant $c_2 > 0$, such that $\forall N, \exists n > N$:

$$\text{Prob}\left[A'(E_{G(1^n)}(Z_n), h(Z_n), 1^n) = f(Z_n)\right] - \text{Prob}\left[A''(h(Z_n), 1^n) = f(Z_n)\right] \geq \frac{1}{n^{c_2}} \qquad (6)$$

(which means that the algorithm A' 'can do better' than any other algorithm which is not given the encryption).

Define the random variable Z_n (not necessarily polynomial) as

$$\text{Prob}(Z_n = \gamma) = \begin{cases} 1/2 & \text{if } \gamma = \alpha_n \\ 1/2 & \text{if } \gamma = \beta_n \\ 0 & \text{otherwise} \end{cases}$$

The function h will be the null function (i.e , A' will use $E_{G(1^n)}(\gamma)$, $1^{|\gamma|}$, and would not need any further information).
The function f:

$$f(\gamma) = \begin{cases} 1 & \text{if } \gamma = \alpha_n \\ 0 & \text{if } \gamma = \beta_n \end{cases}$$

The case in which $\alpha_n = \beta_n$ is not interesting, since in this case, the random variables defined by the computations of A on $\alpha \circ \beta$ and the encryptions of α_n or β_n have the same distribution, which implies that the contradiction assumption would not hold. Thus, we will consider only the case of $\alpha_n \neq \beta_n$, in which f is well defined.

The algorithm A':

Again, A' is actually an infinite sequence $\{A_n'\}$ of polynomial circuits, and since each A_n' is non-uniform it can include in it the string $\alpha_n \circ \beta_n$.

Input: $E_{G(1^n)}(\gamma)$, $1^{|\gamma|}$ ($\gamma \in \{\alpha_n , \beta_n\}$).

A_n' simulates A with the input $\alpha_n \circ \beta_n$, $E_{G(1^n)}(\gamma)$, and outputs its outcome.

We now prove (6) :

$$\text{Prob}\left[A'(E_{G(1^n)}(Z_n)\ ,\ h(Z_n)\ ,\ 1^n) = f(Z_n)\right] =$$

$$= \text{Prob}\,(Z_n = \alpha_n)\cdot\text{Prob}\left[A(\alpha_n \circ \beta_n\ ,\ E_{G(1^n)}(\alpha_n)) = f(\alpha_n)\right] +$$

$$+ \text{Prob}\,(Z_n = \beta_n)\cdot\text{Prob}\left[A(\alpha_n \circ \beta_n\ ,\ E_{G(1^n)}(\beta_n)) = f(\beta_n)\right] =$$

$$= \frac{1}{2}\cdot\text{Prob}\left[A(\alpha_n \circ \beta_n\ ,\ E_{G(1^n)}(\alpha_n)) = 1\right] + \frac{1}{2}\cdot\text{Prob}\left[A(\alpha_n \circ \beta_n\ ,\ E_{G(1^n)}(\beta_n)) = 0\right] =$$

$$= \frac{1}{2}\cdot\left[\text{Prob}\left[A(\alpha_n \circ \beta_n\ ,\ E_{G(1^n)}(\alpha_n)) = 1\right] + 1 - \text{Prob}\left[A(\alpha_n \circ \beta_n\ ,\ E_{G(1^n)}(\beta_n)) = 1\right]\right] =$$

$$= \frac{1}{2} + \frac{1}{2}\cdot\left[\text{Prob}\left[A(\alpha_n \circ \beta_n\ ,\ E_{G(1^n)}(\alpha_n)) = 1\right] - \text{Prob}\left[A(\alpha_n \circ \beta_n\ ,\ E_{G(1^n)}(\beta_n)) = 1\right]\right] \geq \frac{1}{2} + \frac{1}{2\cdot n^{c_1}}$$

(Last inequality follows from the contradiction hypothesis).

Thus, $\exists c_2 > 0\ \forall N,\ \exists n > N$:

$$\text{Prob}\left[A'(E_{G(1^n)}(Z_n)\ ,\ h(Z_n)\ ,\ 1^n) = f(Z_n)\right] \geq \frac{1}{2} + \frac{1}{n^{c_2}}$$

On the other hand, for every polynomial algorithm A'' :

$$\text{Prob}\left[A''(h(Z_n)\ ,\ 1^n) = f(Z_n)\right] \leq \frac{1}{2}$$

since $h(Z_n)$ does not give any information on Z_n , and given only the length n , the random variable Z_n can assume the value α_n or β_n with equal probability. Thus, $f(Z_n)$ can be 0 or 1 with equal probability, and cannot be guessed successfully with a probability greater than ½ (it can be less than ½ since A'' may act 'unreasonably' and output a value that is not in $\{0,1\}$).

Therefore, for every polynomial algorithm A'' : $\exists\, c_2 > 0\ \forall N,\ \exists\, n > N$:

$$\text{Prob}\left[A'(E_{G(1^n)}(Z_n)\ ,\ h(Z_n)\ ,\ 1^n) = f(Z_n)\right] - \text{Prob}\left[A''(h(Z_n)\ ,\ 1^n) = f(Z_n)\right] \geq \frac{1}{2} + \frac{1}{n^{c_2}} - \frac{1}{2} = \frac{1}{n^{c_2}}$$

In contradiction with the scheme being semantically secure.

We conclude that (G,E,D) is secure in the sense of indistinguishability . ■

Proof of Theorem 2 (Uniform case):

The general idea is the same. We will assume that the scheme is not secure in the sense of indistinguishability, and reach a contradiction to the semantic security. In the uniform case, the random variable Z_n

must be polynomial (i.e. samplable by a polynomial algorithm), and A' must be uniform, and thus cannot include any information in it. Instead, the function h is used to provide the required information - the pair (α_n, β_n) .

Assume by contradiction that the scheme is not secure in the sense of indistinguishability . That is, there exist a sequence of polynomial random variables $\{X_n = X_n^{(1)} \circ X_n^{(2)}\}$, a probabilistic polynomial-time algorithm A , and a constant $c > 0$, such that $\forall N,\ \exists\, n > N$, $\exists\, B_n \subseteq \{0,1\}^{2 \cdot n}$:

(1) $\quad \text{Prob}\left[X_n \in B_n\right] > \dfrac{1}{n^c}$

(2) $\quad \forall \alpha \circ \beta \in B_n$:

$$\text{Prob}\left[A\,(\alpha \circ \beta\ ,\ E_{G(1^n)}(\alpha)) = 1\right] - \text{Prob}\left[A\,(\alpha \circ \beta\ ,\ E_{G(1^n)}(\beta)) = 1\right] \geq \frac{1}{n^c}$$

We prove the existence of a sequence of polynomial-time random variables $\{Z_n\}$, a polynomially computable function h , a function f and a polynomial algorithm A' such that for every polynomial algorithm A'' there exists a constant $c > 0$ such that $\forall N,\ \exists\, n > N$:

$$\text{Prob}\left[A'(E_{G(1^n)}(Z_n)\ ,\ h(Z_n)\ ,\ 1^n) = f(Z_n)\right] - \text{Prob}\left[A''(h(Z_n)\ ,\ 1^n) = f(Z_n)\right] \geq \frac{1}{n^c}\ ,$$

contradicting the semantic security.
Here also, any A'' (even one which is not restricted to polynomial running time), given only $h(Z_n)$, will have no information on Z_n or $f(Z_n)$ (which will be one bit), and thus will not be able to output $f(Z_n)$ with a probability greater than ½ .

The definition of Z_n :
Given a string $\alpha \circ \beta \in \{0,1\}^{2 \cdot n}$ it cannot be efficiently decided whether $\alpha \circ \beta$ is in B_n , since no polynomial-time sampling algorithm can distinguish the case

$$\text{Prob}\left[A\,(\alpha \circ \beta\ ,\ E_{G(1^n)}(\alpha)) = 1\right] - \text{Prob}\left[A\,(\alpha \circ \beta\ ,\ E_{G(1^n)}(\beta)) = 1\right] = \frac{1}{n^c}$$

(where $(\alpha \circ \beta) \in B_n$), from the case

$$\text{Prob}\left[A\,(\alpha \circ \beta\ ,\ E_{G(1^n)}(\alpha)) = 1\right] - \text{Prob}\left[A\,(\alpha \circ \beta\ ,\ E_{G(1^n)}(\beta)) = 1\right] = \frac{1}{n^c} - 2^{-n}$$

(i.e. $(\alpha \circ \beta) \notin B_n$). Thus, it will be difficult to create a random variable Z_n ranging over B_n such that $\text{Prob}\,(Z_n = \alpha \circ \beta) = \text{Prob}\,(X_n = \alpha \circ \beta \,|\, X_n \in B_n)$. Instead, we create a random variable Z_n satisfying only $\text{Prob}\,(Z_n \in B_n') > 1 - 2^{-n}$, where

$$B_n' \triangleq \left\{\alpha \circ \beta \,\middle|\, \alpha \circ \beta \in \{0,1\}^{2 \cdot n} \wedge \text{Prob}\left[A\,(\alpha \circ \beta,\ E_{G(1^n)}(\alpha)) = 1\right] - \text{Prob}\left[A\,(\alpha \circ \beta,\ E_{G(1^n)}(\beta)) = 1\right] \geq \frac{1}{2 \cdot n^c}\right\}$$

clearly, $B_n \subseteq B_n{}'$.

The idea is to sample X_n , trying to find a pair $\alpha\circ\beta$ with the largest gap between $\text{Prob}\left[A(\alpha\circ\beta,\ E_{G(1^n)}(\alpha)) = 1\right]$ and $\text{Prob}\left[A(\alpha\circ\beta,\ E_{G(1^n)}(\beta)) = 1\right]$. This pair is very likely to be in $B_n{}'$.

Consider the following sampling algorithm S (which samples pairs mostly in $B_n{}'$):

1. Repeat N_1 times:
   - 1.1 Sample X_n (recall that X_n is a polynomial random variable). Let $\alpha\circ\beta$ be the sampled string.
   - 1.2 Compute N_2 times independently $A(\alpha\circ\beta,\ E_{G(1^n)}(\alpha))$ and $A(\alpha\circ\beta,\ E_{G(1^n)}(\beta))$.
   - 1.3 Estimate, according to the relative frequencies, $\text{Prob}\left[A(\alpha\circ\beta,\ E_{G(1^n)}(\alpha)) = 1\right]$ and $\text{Prob}\left[A(\alpha\circ\beta,\ E_{G(1^n)}(\beta)) = 1\right]$ and calculate the difference between these estimated probabilities.
2. Output the string $\alpha\circ\beta$ for which the difference of the estimated probabilities was maximal (If there are several such strings, one is chosen arbitrarily).

End of algorithm.

Let $T_n \triangleq S(1^n)$.

We will skip here the formal details, but it can be shown, using similar arguments to those used while proving inequality (5), that if N_2 is sufficiently large (fixed polynomial in n^c), then the relative frequencies calculated in step 1.3, estimate quite accurately the real probabilities. Also, if N_1 is large enough, then with a probability which is very close to 1, one of the pairs sampled by S is in B_n and therefore the output pair is in $B_n{}'$. namely,

$$\text{Prob}\,(T_n \in B_n{}') > 1 - 2^{-n}$$

Intuitively, we can think of $B_n{}'$ as a 'safety-zone' surrounding B_n : If we try to sample B_n we might fall outside of B_n , but since this 'safety zone' is wide enough, we are likely to stay inside it, and not fall out of $B_n{}'$ as well.

Let Y_n be a random variable which is uniformly distributed over $\{0,1\}$. For $\gamma = \alpha\circ\beta$ such that $|\alpha| = |\beta| = n$, let $\overline{\gamma} \triangleq \beta\circ\alpha$, and let $\overline{T}_n$ be defined similarly (i.e. to sample $\overline{T}_n$, use the following algorithm: Sample T_n to get a string γ , and output $\overline{\gamma}$).

Z_n will be the following random variable:

$$Z_n \triangleq \begin{cases} 0^n \circ T_n & Y_n = 0 \\ 1^n \circ \overline{T}_n & Y_n = 1 \end{cases}$$

Note that Y_n and T_n are independent.

Y_n and T_n (and also $\overline{T}_n$) are polynomially samplable, and thus, Z_n is a polynomial random variable.

The function h :

$$h(\sigma^n \circ \gamma) = \begin{cases} \gamma & \sigma = 0 \\ \overline{\gamma} & \sigma = 1 \end{cases}$$

thus, if $Z_n = 0^n \circ \alpha \circ \beta$, $h(Z_n) = \alpha \circ \beta$, and if $Z_n = 1^n \circ \beta \circ \alpha$, $h(Z_n) = \alpha \circ \beta$.
In any case, given Z_n , $h(Z_n)$ gives back the value of T_n that generated Z_n .

The function f :

$$f(\sigma^n \circ \gamma) = \sigma$$

The algorithm A' :

Input: $E_{G(1^n)}(\gamma)$, $h(\gamma)$, 1^n , (where $\gamma = \sigma^n \circ \gamma_1 \circ \gamma_2$ such that $|\gamma_1| = |\gamma_2| = n$.)
The algorithm A', using the decomposability condition, computes $E_{G(1^n)}(\gamma_2)$ ($\gamma_2 = \alpha$ or β). Then A' simulates A with the input $E_{G(1^n)}(\gamma_2)$, $h(Z_n)$ ($= \alpha \circ \beta$) and outputs its outcome.

We have,

$$\text{Prob}\left[A'(E_{G(1^n)}(Z_n)\,,\, h(Z_n)\,,\, 1^n) = f(Z_n)\right] =$$

$$= \sum_{\alpha \circ \beta \{0,1\}^{2n}} \text{Prob}\,(T_n = \alpha \circ \beta) \cdot \text{Prob}\left[A'(E_{G(1^n)}(Z_n)\,,\, h(Z_n)\,,\, 1^n) = f(Z_n) \,|\, T_n = \alpha \circ \beta\right] =$$

$$= \sum_{\alpha \circ \beta \in B_n'} \text{Prob}\,(T_n = \alpha \circ \beta) \cdot \text{Prob}\left[A'(E_{G(1^n)}(Z_n)\,,\, h(Z_n)\,,\, 1^n) = f(Z_n) \,|\, T_n = \alpha \circ \beta\right] +$$

$$+ \sum_{\alpha \circ \beta \notin B_n'} \text{Prob}\,(T_n = \alpha \circ \beta) \cdot \text{Prob}\left[A'(E_{G(1^n)}(Z_n)\,,\, h(Z_n)\,,\, 1^n) = f(Z_n) \,|\, T_n = \alpha \circ \beta\right] \geq$$

$$\geq \sum_{\alpha \circ \beta \in B_n'} \text{Prob}\,(T_n = \alpha \circ \beta) \cdot \text{Prob}\left[A'(E_{G(1^n)}(Z_n)\,,\, h(Z_n)\,,\, 1^n) = f(Z_n) \,|\, T_n = \alpha \circ \beta\right] =$$

We will refer in the subsequent computations to a fixed pair $(\alpha, \beta) \in B_n'$. We have

$$\text{Prob}\left[A'(E_{G(1^n)}(Z_n)\,,\, h(Z_n)\,,\, 1^n) = f(Z_n) \,|\, T_n = \alpha \circ \beta\right] =$$

$$= \text{Prob}\,(Y_n = 0) \cdot \text{Prob}\left[A'(E_{G(1^n)}(0^n \circ \alpha \circ \beta)\,,\, h(0^n \circ \alpha \circ \beta)\,,\, 1^n) = f(0^n \circ \alpha \circ \beta)\right] +$$

$$+ \text{Prob}\,(Y_n = 1) \cdot \text{Prob}\left[A'(E_{G(1^n)}(1^n \circ \beta \circ \alpha)\,,\, h(1^n \beta \circ \alpha)\,,\, 1^n) = f(1^n \circ \beta \circ \alpha)\right] =$$

$$= \text{Prob}\,(Y_n = 0) \cdot \text{Prob}\left[A'(E_{G(1^n)}(0^n \circ \alpha \circ \beta)\,,\, \alpha \circ \beta\,,\, 1^n) = 0\right] +$$

$$+ \text{Prob}\,(Y_n = 1) \cdot \text{Prob}\left[A'(E_{G(1^n)}(1^n \circ \beta \circ \alpha)\,,\, \alpha \circ \beta\,,\, 1^n) = 1\right] =$$

$$= \frac{1}{2} \cdot \left[\text{Prob}\left(A(\alpha \circ \beta\,,\, E_{G(1^n)}(\beta)) = 0 \right) + \text{Prob}\left(A(\alpha \circ \beta\,,\, E_{G(1^n)}(\alpha)) = 1 \right) \right] =$$

$$= \frac{1}{2} \cdot \left[1 - \text{Prob}\left(A(\alpha \circ \beta\,,\, E_{G(1^n)}(\beta)) = 1 \right) + \text{Prob}\left(A(\alpha \circ \beta\,,\, E_{G(1^n)}(\alpha)) = 1 \right) \right] =$$

$$= \frac{1}{2} + \frac{1}{2} \cdot \left[\text{Prob}\left(A(\alpha \circ \beta\,,\, E_{G(1^n)}(\alpha)) = 1 \right) - \text{Prob}\left(A(\alpha \circ \beta\,,\, E_{G(1^n)}(\beta)) = 1 \right) \right] \geq \frac{1}{2} + \frac{1}{4 \cdot n^c}$$

(last inequality uses $(\alpha \circ \beta) \in B_n'$).

Thus ,we have

$$\sum_{\alpha \circ \beta \in B_n'} \text{Prob}\,(T_n = \alpha \circ \beta) \cdot \text{Prob}\left(A'(E_{G(1^n)}(Z_n)\,,\, h(Z_n)\,,\, 1^n) = f(Z_n) \,\middle|\, T_n = \alpha \circ \beta \right) \geq$$

$$\geq \sum_{\alpha \circ \beta \in B_n'} \text{Prob}(T_n = \alpha \circ \beta) \cdot \left[\frac{1}{2} + \frac{1}{4 \cdot n^c} \right] =$$

$$= \left[\frac{1}{2} + \frac{1}{4 \cdot n^c} \right] \cdot \text{Prob}\,(T_n \in B_n') \geq \left[\frac{1}{2} + \frac{1}{4 \cdot n^c} \right] \cdot \left(1 - 2^{-n} \right)$$

$$> \frac{1}{2} + \frac{1}{8 \cdot n^c} \qquad \text{(for large enough } n\text{)}.$$

And this implies that: $\exists c' > 0\,,\, \forall N\,,\, \exists\, n > N$:

$$\text{Prob}\left(A'(E_{G(1^n)}(Z_n)\,,\, h(Z_n)\,,\, 1^n) = f(Z_n) \right) \geq \frac{1}{2} + \frac{1}{n^{c'}}$$

Here also, for every polynomial algorithm A'' :

$$\text{Prob}\left(A''(h(Z_n)\,,\, 1^n) = f(Z_n) \right) \leq \frac{1}{2}$$

since given only $\alpha \circ \beta$ (i.e. $h(Z_n)$), Z_n can assume the values $0^n \circ \alpha \circ \beta$ or $1^n \circ \beta \circ \alpha$ with equal probability, and thus $f(Z_n)$ can be 0 or 1 with equal probability and cannot be guessed successfully with a probability greater than ½ . Thus, for every polynomial algorithm A'' : $\exists\, c' > 0$, $\forall N$, $\exists\, n > N$ such that

$$\text{Prob}\left(A'(E_{G(1^n)}(Z_n)\,,\, h(Z_n)\,,\, 1^n) = f(Z_n) \right) - \text{Prob}\left(A''(h(Z_n)\,,\, 1^n) = f(Z_n) \right) \geq \frac{1}{2} + \frac{1}{n^{c'}} - \frac{1}{2} = \frac{1}{n^{c'}}$$

In contradiction with the scheme being semantically secure.

We conclude that (G,E,D) is secure in the sense of indistinguishability . ■

APPENDIX A

Proof of inequality (5):

Namely, assume $(\alpha,\beta) \in D_n^{c_0}$. Then

$$\mathrm{Prob}\left[A''(\alpha\circ\beta,\ E_{G(1^n)}(\alpha)) = 1\right] - \mathrm{Prob}\left[A''(\alpha\circ\beta,\ E_{G(1^n)}(\beta)) = 1\right] \geq \frac{1}{8\cdot n^{c_0}}$$

Proof:

Throughout the proof $n,\ \alpha,\ \beta$ are fixed.

Consider the following notations:

$$\varepsilon \triangleq \frac{1}{n^{c_0}}$$

$$A_\gamma \triangleq A\,(E_{(G(1^n)}(\gamma),\ h(\alpha),\ 1^n) \qquad (\gamma \in \{\alpha,\beta\})$$

$$P_\gamma(v) \triangleq \mathrm{Prob}\,(A_\gamma = v)$$

$\hat{P}_\gamma(v)$ is defined as the relative frequency that v appears as an output of A_γ, as estimated by sampling N times (i.e. by running $A\,(E_{G(1^n)}(\gamma),\ h(\alpha),\ 1^n)$ N times). The intuition is that $\hat{P}_\alpha(v)$ estimates $P_\alpha(v)$ very well.

$$\Delta(v) \triangleq P_\alpha(v) - P_\beta(v)$$

By our assumption $(\alpha,\beta) \in D_n^c$, it follows that there exists v such that $\Delta(v) > \varepsilon$.

$$\hat{\Delta}(v) \triangleq \hat{P}_\alpha(v) - \hat{P}_\beta(v)$$

Thus, $\hat{\Delta}(v)$ is the difference of the relative frequencies, and should estimate the real difference of the probabilities (i.e. $\Delta(v)$).

$$V_1 \triangleq \{\ v : \Delta(v) \geq \frac{\varepsilon}{4}\ \}$$

$$V_2 \triangleq \{\ v : \Delta(v) \geq \varepsilon\ \}$$

(Clearly $V_1 \subseteq V_2 \neq \phi$)

In all subsequent calculations v_0 (which gives the maximal difference of the relative frequencies i.e., the maximal value of $\hat{\Delta}(v)$) is a random variable defined according to the $N = n^{2\cdot c_0+1}$ computations of A''. Hence, v_0 is dependent solely upon A'' and (α,β) .

Now,

$$\text{Prob}\left[A''(\alpha\circ\beta,\, E_{G(1^n)}(\alpha))=1\right]-\text{Prob}\left[A''(\alpha\circ\beta,\, E_{G(1^n)}(\beta))=1\right]=$$

$$=\text{Prob}\,(A_\alpha=v_0)-\text{Prob}\,(A_\beta=v_0)=$$

$$=\text{Prob}\left[A_\alpha=v_0\,|\,v_0\in V_1\right]\cdot\text{Prob}\,(v_0\in V_1)+\text{Prob}\left[A_\alpha=v_0\,|\,v_0\notin V_1\right]\cdot\text{Prob}\,(v_0\notin V_1)$$

$$-\text{Prob}\left[A_\beta=v_0\,|\,v_0\in V_1\right]\cdot\text{Prob}\,(v_0\in V_1)-\text{Prob}\left[A_\beta=v_0\,|\,v_0\notin V_1\right]\cdot\text{Prob}\,(v_0\notin V_1)$$

$$\geq\left[\text{Prob}\left[A_\alpha=v_0\,|\,v_0\in V_1\right]-\text{Prob}\left[A_\beta=v_0\,|\,v_0\in V_1\right]\right]\cdot\text{Prob}\,(v_o\in V_1)-\text{Prob}\,(v_0\notin V_1)$$

Using the bound $\text{Prob}\,(v_0\notin V_1)\leq 8\cdot e^{-\frac{2N\varepsilon^2}{16}}$ proved below, and the definition of V_1 we get

$$\text{Prob}\left[A''(\alpha\circ\beta,\, E_{G(1^n)}(\alpha))=1\right]-\text{Prob}\left[A''(\alpha\circ\beta,\, E_{G(1^n)}(\beta))=1\right]\geq$$

$$\geq\frac{\varepsilon}{4}\cdot\left[1-8\cdot e^{-\frac{2N\varepsilon^2}{16}}\right]-8\cdot e^{-\frac{2N\varepsilon^2}{16}}\geq\frac{\varepsilon}{8}=\frac{1}{8\cdot n^{c_0}}$$

Thus proving inequality (5).

claim: $\text{Prob}\,(v_0\notin V_1)\leq 8\cdot e^{-\frac{2N\varepsilon^2}{16}}$

recall that v_0 gives the maximal difference of the relative frequencies.

$$\text{Prob}\,(v_0\notin V_1)=\text{Prob}\left[v_0\notin V_1\,\middle|\,\hat{\Delta}(v_0)<\frac{\varepsilon}{2}\right]\cdot\text{Prob}\left[\hat{\Delta}(v_0)<\frac{\varepsilon}{2}\right]$$

$$+\text{Prob}\left[v_0\notin V_1\,\middle|\,\hat{\Delta}(v_0)\geq\frac{\varepsilon}{2}\right]\cdot\text{Prob}\left[\hat{\Delta}(v_0)\geq\frac{\varepsilon}{2}\right]$$

$$\leq\text{Prob}\left[\hat{\Delta}(v_0)<\frac{\varepsilon}{2}\right]\tag{A1}$$

$$+\text{Prob}\left[v_0\notin V_1\,\middle|\,\hat{\Delta}(v_0)\geq\frac{\varepsilon}{2}\right]\tag{A2}$$

According to the contradiction assumption, $V_2\neq\phi$. Let $v_2\in V_2$.
According to the definition of v_0, $\hat{\Delta}(v_0)<\frac{\varepsilon}{2}$ implies that for all v, $\hat{\Delta}(v)<\frac{\varepsilon}{2}$ (since v_0 gives the maximal value of $\hat{\Delta}(v)$), in particular : $\hat{\Delta}(v_2)<\frac{\varepsilon}{2}$. Thus,

$$\text{Prob}\left[\hat{\Delta}(v_0)<\frac{\varepsilon}{2}\right]\leq\text{Prob}\left[\hat{\Delta}(v_2)<\frac{\varepsilon}{2}\right]$$

$\hat{\Delta}(v_2) < \frac{\varepsilon}{2}$ implies that $\Delta(v_2) - \hat{\Delta}(v_2) > \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2}$ (since $v_2 \in V_2$ i.e. $\Delta(v) \geq \varepsilon$), and therefore,

$$\text{Prob}\left[\hat{\Delta}(v_2) < \frac{\varepsilon}{2}\right] \leq \text{Prob}\left[\Delta(v_2) - \hat{\Delta}(v_2) > \frac{\varepsilon}{2}\right] .$$

Since

$$\Delta(v_2) - \hat{\Delta}(v_2) = \left[\text{P}_\alpha(v_2) - \hat{\text{P}}_\alpha(v_2)\right] + \left[\hat{\text{P}}_\beta(v_2) - \text{P}_\beta(v_2)\right]$$

(according to the definition of $\Delta(v)$ and $\hat{\Delta}(v)$), it follows that the event ' $\Delta(v_2) - \hat{\Delta}(v_2) > \frac{\varepsilon}{2}$ ' implies the event ' $\text{P}_\alpha(v_2) - \hat{\text{P}}_\alpha(v_2) > \frac{\varepsilon}{4}$ or $\hat{\text{P}}_\beta(v_2) - \text{P}_\beta(v_2) > \frac{\varepsilon}{4}$ ' . Therefore,

$$\text{Prob}\left[\Delta(v_2) - \hat{\Delta}(v_2) > \frac{\varepsilon}{2}\right] \leq \text{Prob}\left[\text{P}_\alpha(v_2) - \hat{\text{P}}_\alpha(v_2) > \frac{\varepsilon}{4}\right] + \text{Prob}\left[\hat{\text{P}}_\beta(v_2) - \text{P}_\beta(v_2) > \frac{\varepsilon}{4}\right]$$

We will bound from above each of the components in the right side of the last inequality:
We define N $0-1$ random variables $x_1^\alpha \cdots x_N^\alpha$ as follows (recall that N is the number of the computations of $A\,(E_{G(1^n)}(\alpha),\, h\,(\alpha),\, 1^n)$ and $A\,(E_{G(1^n)}(\beta),\, h\,(\alpha),\, 1^n)$, as described in step I of algorithm A''):

$x_i^\alpha = 1$ iff the i'th computation of $A\,(E_{G(1^n)}(\alpha),\, h\,(\alpha),\, 1^n)$ yields value v_2 .

These N computations of $A\,(E_{G(1^n)}(\alpha),\, h\,(\alpha),\, 1^n)$ are independent and therefore, $x_1^\alpha \cdots x_N^\alpha$ are independent random variables. Thus, we can use Chernoff bound to obtain:

$$\text{Prob}\left[P_\alpha(v_2) - \hat{P}_\alpha(v_2) \geq \frac{\varepsilon}{2}\right] \leq 2 \cdot e^{-\frac{2N\varepsilon^2}{16}}$$

The random variables x_i^β $(1 \leq i \leq N)$ are defined similarly, and using the same arguments, we get the same upper bound for the second component. Intuitively, these bounds indicate that the estimations $\hat{P}_\alpha(v_2)$ and $\hat{P}_\beta(v_2)$ of the real probabilities $P_\alpha(v_2)$ and $P_\beta(v_2)$ were quite accurate.

Thus,

$$\text{Prob}\left[\hat{\Delta}(v_0) < \frac{\varepsilon}{2}\right] \leq 4 \cdot e^{-\frac{2N\varepsilon^2}{16}} \qquad (*)$$

which bounds (A1). We will prove now that (A2) is bounded similarly.

The event ' $v_0 \notin V_1$ given $\hat{\Delta}(v_0) > \frac{\varepsilon}{2}$ ' implies the event ' $\hat{\Delta}(v_0) - \Delta(v_0) > \frac{\varepsilon}{2} - \frac{\varepsilon}{4} = \frac{\varepsilon}{4}$ ' (since according to the definition of V_1 , $\Delta(v_0) < \frac{\varepsilon}{4}$)

Using the same arguments as before, we obtain that:

$$\text{Prob}\left(v_0 \notin V_1 \,\middle|\, \hat{\Delta}(v_0) > \frac{\varepsilon}{2}\right) \leq 4 \cdot e^{-\frac{2N\varepsilon^2}{16}} \qquad (**)$$

Bounding (A1) and (A2) according to (*) and (**) respectively, we conclude that

$$\text{Prob}\,(v_0 \notin V_1) \leq 8 \cdot e^{-\frac{2N\varepsilon^2}{16}} \qquad \square$$