Τελικό Διαγώνισμα Κρυπτογραφία

Επώνυμο :
Όνομα :
Α.Μ.:

[Με Λύσεις]

Οδηγίες : Κάθε θέμα είναι 2.5 βαθμοί. Ένα θέμα κενό (εντελώς λευκή σελίδα) είναι 0.5 βαθμοί. Μία εντελώς άσχετη απάντηση σε ένα θέμα είναι 0 βαθμοί. Έτσι π.χ. κάποιος μπορεί να πάρει 5 με μία τέλεια απάντηση (2.5) και μία που πιάνει το 60%.

Άσκηση 1

Έστω το εξής κρυπτοσύστημα $\langle \mathcal{G}, \mathcal{E}, \mathcal{D} \rangle$: η $\mathcal{G}$ με είσοδο 1^k παράγει το δημόσιο κλειδί $\langle n, e, H(\cdot) \rangle$, όπου n k-bit σύνθετος και το μυστικό κλειδί $\langle d, p, q \rangle$. Ισχύει ότι $e \cdot d = 1 \bmod \phi(n)$, $n = pq$ (όπως στο RSA) καθώς και $H : \mathbb{Z}_n \to \{0,1\}^k$ είναι μια συνάρτηση κατακερματισμού (hash). Η συνάρτηση $\mathcal{E}$ με είσοδο $M \in \{0,1\}^k$ επιστρέφει την τιμή $\langle r^e \bmod n, H(r) \oplus M \rangle$ όπου $\oplus$ συμβολίζει την πράξη exclusive-or μεταξύ δυαδικών συμβολοακολουθιών. Για την απόδειξη, φανταζόμαστε ότι το $H : \mathbb{Z}_n^* \to \{0,1\}^k$ λειτουργεί σαν τυχαίο μαντείο.

(1) Διατυπώστε την υπόθεση RSA και το μοντέλο ασφάλειας IND-CPA.

(2) Περιγράψτε πως πιστεύετε οτι πρέπει να δουλεύει η διαδικασία της αποκρυπτογράφησης $\mathcal{D}$.

(3) Δείξετε ότι το κρυπτοσύστημα ικανοποιεί ασφάλεια τύπου IND-CPA στο μοντέλο τυχαίου μαντείου κάτω από την υπόθεση RSA.

Λύση.

(1) Έστω $n = pq$ όπου p, q πρώτοι αριθμοί μεγέθους $\lambda/2$ bits. Ένας αλγόριθμος για το πρόβλημα RSA λειτουργεί με είσοδο $\langle n, y, e, \rangle$ και επιτυγχάνει ότι επιστρέφει z τέτοιο ώστε $z^e = y \bmod n$. Η υπόθεση RSA λέει ότι δεν υπάρχει αλγόριθμος για το πρόβλημα RSA που να λειτουργεί σε πολυωνυμικό χρόνο στο λ με πιθανότητα μη αμελητέα στο λ.

Το μοντέλο ασφάλειας IND-CPA διατυπώνεται σαν ένα παιχνίδι G που παίζεται με έναν αντίπαλο $\mathcal{A}$ σε σχέση με ένα κρυπτογραφικό σύστημα $\langle \text{Gen}, \text{Enc}, \text{Dec} \rangle$ δημοσίου κλειδιού. Στο παιχνίδι πρώτα υπολογίζεται το $(pk, sk) \leftarrow \text{Gen}(1^\lambda)$ και ο αντίπαλος παίρνει την είσοδο pk. Ο αντίπαλος διαλέγει δύο μυνήματα m_0, m_1 καθώς και μία βοηθητική τιμή aux. Μία τυχαία τιμή $b \in \{0,1\}$ διαλέγεται και ο αντίπαλος παίρνει σαν είσοδο τα (aux, c) όπου $c \leftarrow \text{Enc}(pk, m_b)$. Ο αντίπαλος τερματίζει με μία έξοδο b^*. Το παιχνίδι τερματίζει με την τιμή 1 σε περίπτωση που $b = b^*$, αλλιώς με την τιμή 0. Ο αντίπαλος κερδίζει το παιχνίδι με πλεονέκτημα α άν ισχύει $\mathbf{Prob}[G^{\mathcal{A}}(1^\lambda) = 1] \geq 1/2 + \alpha$. Ένα κρυπτοσύστημα είναι ασφαλές στο μοντέλο ασφάλειας IND-CPA αν ισχύει ότι για κάθε πολυωνυμικά φραγμένο αντίπαλο $\mathcal{A}$ το πλεονέκτημα α να νικήσει το παιχνίδι είναι αμελητέο.

(2) Η διαδικασία κρυπτογράφησης $\mathcal{D}$ λειτουργεί ως εξής : $\mathcal{D}(d, n, \langle y, z \rangle) = z \oplus (H(y^d \bmod n))$. Πράγματι άν $y = r^e \bmod n$ και $z = H(r) \oplus M$ ισχύει ότι

$$z \oplus H(y^d \bmod n) = H(r) \oplus M \oplus H(r^{ed} \bmod n) = H(r) \oplus M \oplus H(r) = M$$

(3) Περιγράφουμε ένα αλγόριθμο $\mathcal{B}$ που λύνει το πρόβλημα RSA βάσει ενός αντιπάλου IND-CPA για το παραπάνω κρυπτοσύστημα στο μοντέλο τυχαίου μαντείου. Στο μοντέλο τυχαίου μαντείου ισχύει ο αντίπαλος $\mathcal{A}$ έχει πρόσβαση στη συνάρτηση $H(\cdot)$ σαν μαντείο το οποίο μπορούμε να το προσομοιώσουμε κατά τη διάρκεια της εκτέλεσης παιχνιδιού προς ώφελος μας. Ο $\mathcal{B}$ με είσοδο (n, y, e) θέτει το $pk = (n, e)$ και ξεκινά τον $\mathcal{A}$. Ο $\mathcal{B}$ προσομοιώνει το τυχαίο μαντείο ως εξής : για κάθε ερώτηση r ελέγχεται αν $r^e = y \bmod n$. Αν αυτό ισχύει ο $\mathcal{B}$ τερματίζει επιστρέφοντας r. Αλλιώς ελέγχεται αν το ζεύγος (r, h) υπάρχει στον πίνακα H. Αν όχι τότε διαλέγεται τιμή h τυχαία από το $\mathbb{Z}_n$ και εισάγεται το ζεύγος (r, h) στον πίνακα h. Σε κάθε περίπτωση επιστρέφεται το h. Ο $\mathcal{A}$ επιστρέφει την τιμή (aux, m_0, m_1). Ο $\mathcal{B}$ διαλέγει το b τυχαία και θέτει $c = (y, u \oplus m_b)$ όπου u διαλέγεται τυχαία από το $\{0,1\}^k$. Ο $\mathcal{A}$ λαμβάνει τα (aux, c) και η προσομοίωση του συνεχίζεται από τον $\mathcal{B}$ μέχρι τέλους. Παρατηρούμε ότι το u δεν χρησιμοποιείται από τον $\mathcal{B}$ σε καμμία περίπτωση πέρα από την επιλογή του c.

Έστω α το πλεονέκτημα του $\mathcal{A}$ να κερδίσει το παιχνίδι IND-CPA. Έστω WIN το γεγονός ότι ο $\mathcal{B}$ λύνει το RSA. Το γεγονός αυτό είναι ακριβώς το γεγονός όταν ο $\mathcal{A}$ ρωτάει στο μαντείο την τιμή $y^{1/e} \bmod n$. Παρατηρούμε ότι όταν ο $\mathcal{A}$ δεν ρωτάει αυτήν τιμή μπορεί να μαντέψει σωστά με πιθανότητα ακριβώς $1/2$. Δηλαδή $\mathbf{Prob}[G = 1 \mid \neg\text{WIN}] = 1/2$. Επίσης χωρίς βλάβη της γενικότητας μπορούμε να πούμε ότι ο $\mathcal{A}$ πάντοτε μαντεύει σωστά όταν το WIN συμβαίνει. Αφού ισχύει $\mathbf{Prob}[G = 1] \geq 1/2 + \alpha$ έχουμε και ότι $\mathbf{Prob}[G = 1 \wedge \text{WIN}] + \mathbf{Prob}[G = 1 \wedge \neg\text{WIN}] \geq 1/2 + \alpha$, άρα $\mathbf{Prob}[\text{WIN}] + \mathbf{Prob}[\neg\text{WIN}]/2 \geq 1/2 + \alpha$ που δίνει ότι $\mathbf{Prob}[\text{WIN}] \geq \alpha$. Έτσι δείξαμε ότι ο αλγόριθμος $\mathcal{B}$ επιτυγχάνει με πιθανότητα α ίση με το πλεονέκτημα του $\mathcal{A}$ στο παιχνίδι IND-CPA.

Επώνυμο :
Όνομα :
Α.Μ.:

Άσκηση 2

Έχετε τρία νομίσματα από τα οποία τα δύο είναι κίβδηλα. Ένα κίβδηλο επιστρέφει γράμματα με πιθανότητα $0 < \alpha < 1/2$ ενώ το άλλο επιστρέφει γράμματα με πιθανότητα $1-\alpha$. Το τρίτο νόμισμα είναι γνήσιο και επιστρέφει γράμματα με πιθανότητα $1/2$. Τα νομίσματα είναι αδιαχώριστα 'με το μάτι.'

(1) Δώστε τον τύπο της στατιστικής απόστασης μεταξύ δύο πιθανοτικών κατανομών.

(2) Περιγράψτε έναν αλγόριθμο που τερματίζει πάντοτε και που χρησιμοποιεί τα τρία νομίσματα με τις ελάχιστες δυνατές ρίψεις ώστε να επιστρέψει έξοδο που είναι ομοιόμορφα κατανεμημένη στο $\{0,1\}$. Αν δεν μπορείτε να βρείτε τέτοιο αλγόριθμο δώστε έναν αλγόριθμο που τερματίζει πάντοτε και πλησιάζει την ομοιόμορφη κατανομή όσο καλύτερα γίνεται (με τη έννοια της στατιστικής απόστασης). Σε κάθε περίπτωση δώστε πλήρη αιτολόγηση της απάντησης σας. Σημείωση : ο αλγόριθμος σας δεν πρέπει να χρησιμοποιεί άλλη πηγή τυχαιότητας πέρα από τα τρία νομίσματα.

Λύση.

(1) Ο τύπος της στατιστικής απόστασης είναι ο εξής :

$$\frac{1}{2} \cdot \sum_{a \in D} |\mathbf{Prob}[X = a] - \mathbf{Prob}[Y = a]|$$

Στην παραπάνω έκφραση το a τρέχει πάνω σε όλα τα πιθανά μέλη του πεδίου D και οι X, Y είναι τυχαίες μεταβλητές πάνω στο D.

(2) Ένας τρόπος λύσης είναι να δώσουμε σαν έξοδο το $y = b_1b_2 + b_2b_3 + b_1b_3 \bmod 2$ όπου b_i είναι η τυχαία μεταβλητή που αντιστοιχεί στο νόμισμα i. Πράγματι σε αυτήν την περίπτωση έχουμε ότι η πιθανότητα το $y = 1$ είναι $1/2$ κάτι που μπορεί να υπολογιστεί ως εξής : χωρίς βλάβη της γενικότητας τα κίβδηλα νομίσματα είναι τα $i = 1, 2$. Οι περιπτώσεις να έρθει 1 είναι οι εξής

b_1	b_2	b_3	Πιθανότητα
1	1	0	$\alpha(1-\alpha)1/2 = \alpha/2 - \alpha^2/2$
0	1	1	$(1-\alpha)(1-\alpha)1/2 = 1/2 + \alpha^2/2 - \alpha$
1	0	1	$\alpha^2/2$
1	1	1	$\alpha(1-\alpha)1/2 = \alpha/2 - \alpha^2/2$

Έτσι έχουμε $\mathbf{Prob}[y = 1] = \alpha(1-\alpha) + 1/2 + \alpha^2 - \alpha = 1/2$.

Επώνυμο :
Όνομα :
Α.Μ.:

Άσκηση 3

(1) Να ορίσετε τι είναι ένα πρωτόκολλο μηδενικής γνώσης για μία γλώσσα $\mathcal{L} = \{x \mid \exists w : R(x, w) = 1\}$ (όπου R πολυωνυμικός αλγόριθμος με έξοδο στο $\{0, 1\}$) δίνοντας τις τρεις ιδιότητες : πληρότητα (completeness), ορθότητα (soundness), μηδενική γνώση (zero-knowledge). Να δώσετε μόνο τη 'μαθηματική διατύπωση' των ιδιοτήτων - εξηγήσεις 'υψηλού επιπέδου'/περιγραφικές στα Ελληνικά δεν χρειάζονται και θα προσμετρηθούν αρνητικά. Επίσης να εξηγήσετε τι σημαίνει η ιδιότητα μηδενικής γνώσης για τίμιους επαληθευτές (honest verifier zero-knowledge).

(2) Να αποδείξετε οτι το παρακάτω πρωτόκολλο είναι πρωτόκολλο μηδενικής γνώσης για τίμιους επαληθευτές για το διακριτό λογάριθμο x του h βάσει του g στην υποομάδα $\langle g \rangle$ τάξης m της G. (Δηλαδή πρέπει να δείξετε τις τρεις ιδιότητες).

1. Ο prover διαλέγει τυχαία $\rho_1, \ldots, \rho_k$ από το $\mathbb{Z}_m$ και στέλνει τα $\langle y_1, \ldots, y_k \rangle = \langle g^{\rho_1}, \ldots, g^{\rho_k} \rangle$ στον verifier.
2. Ο verifier διαλέγει k bits $b_1, \ldots, b_k$ τυχαία και τα στέλνει στον prover.
3. Ο prover στέλνει στον verifier τις τιμές t_j που ορίζονται σαν $t_j = \rho_j$ αν $b_j = 0$ και $t_j = \rho_j + x$ αν $b_j = 1$.
4. Ο verifier ελέγχει για κάθε $j \in \{1, \ldots, k\}$, αν ισχύει το $(b_j = 0) \rightarrow (g^{t_j} = y_j)$ και αν ισχύει το $(b_j = 1) \rightarrow (g^{t_j} = y_j h)$.

Στην επιχειρηματολογία που θα παραθέσετε μπορείτε να υποθέσετε οτι είναι γνωστό το ακόλουθο (που έχουμε δείξει): αν ένας (κακός) prover είναι πειστικός στον verifier με πιθανότητα α τότε με ένα μόνο rewinding επιτυγχάνουμε δύο πειστικές conversations που έχουν διαφορετική δεύτερη κίνηση με πιθανότητα τουλάχιστον $\alpha^2/4 - 2^{-k}$.

Λύση.

(1) Για την απάντηση βλέπε τις σημειώσεις του μαθήματος.

(2) Για την πληρότητα έχουμε ότι ισχύει πάντοτε. Πράγματι, αν $b_j = 0$ έχουμε $g^{t_j} = g^{\rho_j} = y_j$ και αν $b_j = 1$ έχουμε $g^{t_j} = g^{\rho_j + x} = y_j h$ για όλα τα $j = 1, \ldots, k$.

Για την ορθότητα έχουμε το εξής : έστω δύο conversations με την ίδια πρώτη κίνηση και διαφορετικές δεύτερες κινήσεις $\langle y_1, \ldots, y_k, b_1, \ldots, b_k, t_1, \ldots, t_k \rangle$ και $\langle y_1, \ldots, y_k, b_1^*, \ldots, b_k^*, t_1^*, \ldots, t_k^* \rangle$. Έτσι έχουμε ότι υπάρχει j τέτοιο ώστε $b_j \neq b_j^*$. Χωρίς βλάβη της γενικότητας έστω ότι $b_j = 0$ και $b_j^* = 1$. Αυτό σημαίνει ότι μπορούμε να υπολογίσουμε το $x = t_j^* - t_j$. Έτσι αφού μπορούμε να επιτύχουμε δυο τέτοιες conversations με πιθανότητα $\alpha^2/4 - 2^{-k}$ μπορούμε και να υπολογίσουμε το x με την ίδια πιθανότητα.

Για την ιδιότητα της μηδενικής γνώσης για τίμιους επαληθευτές έχουμε το εξής : έστω η επόμενη κατασκευή conversations μεταξύ prover και verifier :

$$\langle g^{t_1} h^{-b_1}, \ldots, g^{t_k} h^{-b_k}, b_1, \ldots, b_k, t_1, \ldots, t_k \rangle$$

όπου τα $b_1, \ldots, b_k$ διαλέγονται τυχαία από το $\{0, 1\}$ και τα $t_1, \ldots, t_k$ διαλέγονται τυχαία από το $\mathbb{Z}_m$.

Η παραπάνω τυχαία μεταβλητή έχει την ίδια κατανομή με την τυχαία μεταβλητή που παράγεται στις conversations μεταξύ του τίμιου prover και του τίμιου verifier.

Επώνυμο:
Όνομα:
Α.Μ.:

Άσκηση 4

Η Αλίκη και ο Βασίλης θέλουν να στρίψουν ένα νόμισμα μέσω Internet. Θέλουν να βρούν ένα πρωτόκολλο έτσι ώστε στο τέλος του πρωτοκόλλου να λάβουν ένα bit έτσι ώστε το αποτέλεσμα να είναι κατανεμημένο στο $\{0,1\}$ ομοιόμορφα ακόμη και αν ένας από τους δύο παίκτες δεν ακολουθεί το πρωτόκολλο. Η Αλίκη προτείνει το εξής πρωτόκολλο στο Βασίλη:

1. Η Αλίκη στο πρώτο βήμα διαλέγει μια πολλαπλασιαστική ομάδα G, ένα στοιχείο g τάξης m όπου m πρώτος αριθμός και στέλνει στο Βασίλη τα $\langle G, g, h, m\rangle$ όπου h είναι τυχαίο στοιχείο του $\langle g\rangle$.
2. Ο Βασίλης ελέγχει ότι το m είναι πρώτος αριθμός καθώς και ότι το $g^m = 1$ και $g \neq 1$. Ο Βασίλης διαλέγει $b \in \{0,1\}$ τυχαία και στέλνει στην Αλίκη το στοιχείο $c = g^r h^b$ με r τυχαίο στοιχείο του $\mathbb{Z}_m$.
3. Η Αλίκη καταγράφει το c και στέλνει στο Βασίλη το b' όπου $b' \in \{0,1\}$ το διαλέγει τυχαία.
4. Ο Βασίλης στέλνει στην Αλίκη τα στοιχεία r, b και τερματίζει επιστρέφοντας $(b + b') \bmod 2$.
5. Η Αλίκη ελέγχει ότι $c = g^r h^b$ και $b \in \{0,1\}$ και εάν ισχύει τερματίζει επιστρέφοντας $(b + b') \bmod 2$. Στην άλλη περίπτωση ($c \neq g^r h^b$) η Αλίκη τερματίζει επιστρέφοντας fail.

Να δείξετε τα εξής : (1) Ακόμη και αν η Αλίκη δεν ακολουθεί το πρωτόκολλο, ο Βασίλης, ακολουθώντας το πρωτόκολλο πιστά, είναι σίγουρος ότι η τιμή με την οποία τερματίζει είναι κατανεμημένη τυχαία στο $\{0,1\}$. Υπόδειξη: Για να δικαιολογήσετε την απάντηση σας μπορείτε να υποθέσετε μια οποιαδήποτε συναρτησιακή σχέση $f_A : \langle g\rangle \to \{0,1\}$ που μπορεί να έχει το b' με το c (δηλαδή η f_A αντιπροσωπεύει τον τρόπο που η Αλίκη διαλέγει το b' βάσει του c) και να δείξετε ότι η έξοδος του Βασίλη (που τώρα είναι $(f_A(c) + b) \bmod 2$) εξακολουθεί να είναι τυχαία κατανεμημένη στο $\{0,1\}$. (2) Σε περίπτωση που ο Βασίλης δεν ακολουθεί το πρωτόκολλο, ας υποθέσουμε ότι ο Βασίλης χρησιμοποιεί το πρόγραμμα B το οποίο λειτουργεί σε δύο στάδια ως εξής : με είσοδο $\langle G, g, h, m\rangle$ δίνει ένα c (η πρώτη κίνηση του Βασίλη) και κατόπιν με είσοδο b' επιστρέφει τα r, b (η δεύτερη κίνηση του Βασίλη). Έστω το γεγονός OK ότι το πρόγραμμα B περνάει τον έλεγχο της Αλίκης όταν αυτή ακολουθεί το πρωτόκολλο. Υποθέτουμε ότι $Pr[\text{OK}] = 1$ δηλαδή το πρόγραμμα B απαντάει πάντοτε με τρόπο που Αλίκη δεν κάνει fail.

Έστω ότι το πρόγραμμα B όταν επικοινωνεί με την Αλίκη (που παίζει τίμια) την κάνει να επιστρεψει 1 με πιθανότητα $3/4$, δηλαδή $Pr[(b + b') \bmod 2 = 1] = 3/4$, και έτσι η Αλίκη **δεν εξάγει** ένα τίμιο νόμισμα. Ας υποθέσουμε $Pr[b = 1|b' = 0] = \alpha$. (2α) Τι πρέπει να ικανοποιεί το α ; (2β) Με τι πρέπει να είναι ίση η δεσμευμένη πιθανότητα $Pr[b = 0|b' = 1]$; (2γ) Χρησιμοποιώντας το πρόγραμμα B να κατασκευάσετε πρόγραμμα B^* που να λύνει το πρόβλημα του διακριτού λογαρίθμου στην στην ομάδα $\langle g\rangle$ δηλαδή με είσοδο g, h να επιστρέφει x τέτοιο ώστε $h = g^x$. Με αυτό τον τρόπο συμπεραίνουμε ότι το πρωτόκολλο επιτρέπει και στην Αλίκη να είναι σίγουρη ότι και ο Βασίλης δεν μπορεί να κλέψει (αν πιστεύει στη δυσκολία του διακριτού λογαρίθμου).

Λύση. (1) Έστω η έξοδος του Βασίλη είναι η τυχαία μεταβλητή $u = f_A(c) + b$. Θέλουμε να υπολογίσουμε την πιθανότητα $u = 1$. Έστω ζεύγος (c, b) που κάνει τη μεταβλητή $u = 1$. Παρατηρούμε ότι $c = g^r h^b = g^{r+(2b-1)\cdot \log_g h} h^{1-b} = g^{r'} h^{1-b}$. Αυτό σημαίνει ότι για κάθε επιλογή του Βασίλη για τα (r, b) που τον οδηγεί στο να βγάλει το αποτέλεσμα 1 υπάρχει μια ακριβώς επιλογή $(r', 1-b)$ που τον οδηγεί στο να βγάλει το αποτέλεσμα $u' = f_A(c) + 1 - b = 0$. Έπεται ότι η πιθανότητα του γεγονότος $u = 1$ είναι $1/2$.

(2) Έστω οτι η έξοδος της Αλίκης είναι 1 με πιθανότητα $3/4$. Αυτό σημαίνει ότι $P[b+b' = 1] = 3/4$. Δεδομένου ότι η Αλίκη διαλέγει το b' ομοιόμορφα πάνω στο $\{0,1\}$ έχουμε ότι έχουμε ότι το b θα πρέπει να σχετίζεται με το b' ώστε άν $P[b = 1|b' = 0] = \alpha$ τότε $P[b = 0|b' = 1] = 3/2 - \alpha$ και $\alpha \geq 1/2$. Πράγματι έχουμε

$$P[b+b' = 1] = P[b+b' = 1|b' = 0]P[b' = 0]+P[b+b' = 1|b' = 1]P[b' = 1] = (P[b = 1|b' = 0]+P[b = 0|b' = 1])/2 = 3/4$$

Αυτό απαντάει τις ερωτήσεις (α), (β).

(γ) Έστω το εξής πρόγραμμα B^* με είσοδο το $\langle G, g, h, m\rangle$: Πρώτα τρέχουμε το προγραμμα B με $\langle G, g, h, m\rangle$ σαν είσοδο και παίρνουμε το c. Μετά δίνουμε $b' = 0$ και παίρνουμε τα r, b. Κανουμε rewind με $b' = 1$ και παίρνουμε τα r^*, b^*. Αν ισχύει $(r, b) = (r^*, b^*)$ τερματίζουμε. Αλλιώς έχουμε ότι $g^r h^b = g^{r^*} h^{b^*}$ ή ισοδύναμα $g^{r-r^*} = h^{b^*-b}$. Αν ισχύει ότι $b = b^*$ τότε και αναγκαστικά $r = r^*$, άρα $b \neq b^*$, έστω χωρίς βλάβη της γενικότητας ότι $b = 0, b^* = 1$. Από αυτό έχουμε ότι $h = g^{r-r^*}$ άρα υπολογίσαμε το διακριτό λογάριθμο του h βάσει το g.

Οπότε έχουμε ότι όταν δίνουμε $b' = 0$ στο πρόγραμμα B έχουμε ότι με πιθανότητα $\alpha \geq 1/2$ προσλαμβάνουμε την έξοδο (r, b) με $b = 1$. Κάνοντας rewind δίνοντας $b' = 1$ στο πρόγρμμα B έχουμε ότι η πιθανότητα να πάρουμε απάντηση με (r^*, b^*) με $b^* = 0$ είναι $3/2 - \alpha$. Τελικά με πιθανότητα $\alpha(3/2 - \alpha)$ προσλαμβάνουμε τις δύο διαφορετικές απαντήσεις και κατασκευάζουμε το διακριτό λογάριθμο $\log_g h$.