PSEUDORANDOM GENERATORS- PREDICATES & ZK PROOFS

ΑΛΓΟΡΙΘΜΟΙ ΚΑΙ ΠΟΛΥΠΛΟΚΟΤΗΤΑ 2

Επιμέλεια: Νικόλαος Λάμπρου

μΠλΑ 2014

Γεννήτρια ψευδοτυχαίων αριθμών

- Άτυπος ορισμός: Έστω μια συνάρτηση G από strings σε strings.Λέμε ότι η G είναι γεννήτρια ψευδοτυχαίων αριθμών αν από τυχαία strings μήκους m μπορεί να παράγει "τυχαία" strings μήκους *l*>m.

Γεννήτρια ψευδοτυχαίων αριθμών

- Άτυπος ορισμός: Έστω μια συνάρτηση G από strings σε strings.Λέμε ότι η G είναι γεννήτρια ψευδοτυχαίων αριθμών αν από τυχαία strings μήκους m μπορεί να παράγει "τυχαία" strings μήκους *l*>m.
- Έχουν πολλές εφαρμογές στην κρυπτογραφία (κυρίως σαν υπορουτίνα πρωτοκόλλων)

Γεννήτρια ψευδοτυχαίων αριθμών

- Ορισμός : Μια συνάρτηση G από το $\{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ λέμε ότι είναι ψευδογεννήτρια τυχαίων αριθμών αν είναι δύσκολο να "διαχωρίσεις" αν οι τιμές της προέρχονται από την G η από την U_l.

Γεννήτρια ψευδοτυχαίων αριθμών

- Ορισμός : Μια συνάρτηση G από το $\{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ λέμε ότι είναι ψευδογεννήτρια τυχαίων αριθμών αν είναι δύσκολο να "διαχωρίσεις" αν οι τιμές της προέρχονται από την G η από την U_l.
- Δηλαδή για ppt αλγόριθμο διαχωρισμού A να ισχύει:

$$|Pr[A(G(U_n))=1]-Pr[A(U_l)=1]<neg(1^n)$$

Γεννήτρια ψευδοτυχαίων αριθμών

- Ορισμός : Μια συνάρτηση G από το $\{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ λέμε ότι είναι ψευδογεννήτρια τυχαίων αριθμών αν είναι δύσκολο να "διαχωρίσεις" αν οι τιμές της προέρχονται από την G η από την U_l.
- Δηλαδή για ppt αλγόριθμο διαχωρισμού A να ισχύει:

$|Pr[A(G(U_n))=1]-Pr[A(U_l)=1]<neg(1^n)$

Αλλιώς για οποιοδήποτε στατιστικό test πολυωνυμικού χρόνου η απόσταση να είναι αμελητέα.

Ορισμοί

- Έστω δυο τυχαίες κατανομές X,Y.Ορίζουμε την στατιστική τους απόσταση ως:
- $D(X,Y)=\frac{1}{2}(\Sigma\ |Pr(X=k)-Pr(Y=k)|)$

Ορισμοί

- Έστω δυο τυχαίες κατανομές X,Y.Ορίζουμε την στατιστική τους απόσταση ως:
- $D(X,Y)=\frac{1}{2}(\Sigma\ |Pr(X=k)-Pr(Y=k)|)$
- Ορίζουμε ως στατιστικό test η αλγόριθμο διαχωρισμού A (δεν μας ενδιαφέρει να είναι πολυωνυμικός)
- $|Pr(A(x)=1)-Pr(A(y)=1)| \leq D(X,Y)$

Ορισμοί

- Έστω δυο τυχαίες κατανομές X,Y.Ορίζουμε την στατιστική τους απόσταση ως:
- $D(X,Y)=\frac{1}{2}(\Sigma\ |Pr(X=k)-Pr(Y=k)|)$
- Ορίζουμε ως στατιστικό test η αλγόριθμο διαχωρισμού A (δεν μας ενδιαφέρει να είναι πολυωνυμικός)
- $|Pr(A(x)=1)-Pr(A(y)=1)| \leq D(X,Y)$
- Αυτό μας περιγράφει την επιτυχία του A να καταλάβει από πια κατανομή εμφανίζεται η τιμή και το καλύτερο που μπορεί να φτάσει είναι η στατιστική απόσταση τον τιμών.

Unpredictability

- Ορισμός: Μια συνάρτηση G από το $\{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ λέμε ότι είναι unpredictable αν μας δώσουν μια ακολουθία της εικόνας του string τις και εμείς δεν μπορούμε να προσδιορίσουμε το επόμενο bit της.

Unpredictability

- Ορισμός: Μια συνάρτηση G από το $\{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ λέμε ότι είναι unpredictable αν μας δώσουν μια ακολουθία της εικόνας του string τις και εμείς δεν μπορούμε να προσδιορίσουμε το επόμενο bit της.
- Δηλαδή στην καλύτερη να διαλέξουμε τυχαία! Πιο αναλυτικά:

Unpredictability

- Ορισμός: Μια συνάρτηση G από το $\{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ λέμε ότι είναι unpredictable αν μας δώσουν μια ακολουθία της εικόνας του string τις και εμείς δεν μπορούμε να προσδιορίσουμε το επόμενο bit της.
- Δηλαδή στην καλύτερη να διαλέξουμε τυχαία! Πιο αναλυτικά:
- Για κάθε πιθανοτικό πολυωνιμικό αλγόριθμο Β,η πιθανότητα να βρει το επόμενο bit είναι το πολύ ½ και κάτι αμελητέο.
- $Pr[B(1^n,y_1,y_2,..,y_{i-1})=y_i]<=1/2+neg(1^n)$

Το unpredictability είναι ασφαλές κάτω από την υπόθεση του psedorandomness

- Υποθέτοντας ότι υπάρχει A ppt τω να μπορεί να προβλέψει το επόμενο bit με πιθανότητα ½ + κάτι μη αμελητέο, τότε μπορούμε να τον χρησιμοποιήσουμε για να διακρίνουμε αν κάτι είναι τυχαίο η ψευδοτυχαίο με πιθανότητα μη αμελητέα.

Το unpredictability είναι ασφαλές κάτω από την υπόθεση του psedorandomness

- Υποθέτοντας ότι υπάρχει A ppt τω να μπορεί να προβλέψει το επόμενο bit με πιθανότητα ½ + κάτι μη αμελητέο, τότε μπορούμε να τον χρησιμοποιήσουμε για να διακρίνουμε αν κάτι είναι τυχαίο ή ψευδοτυχαίο με πιθανότητα μη αμελητέα.
- B κάνει το εξής:
- 1)Διάβασε το input μέχρι το i-1.

Το unpredictability είναι ασφαλές κάτω από την υπόθεση του psedorandomness

- Υποθέτοντας ότι υπάρχει A ppt τω να μπορεί να προβλέψει το επόμενο bit με πιθανότητα ½ + κάτι μη αμελητέο, τότε μπορούμε να τον χρησιμοποιήσουμε για να διακρίνουμε αν κάτι είναι τυχαίο ή ψευδοτυχαίο με πιθανότητα μη αμελητέα.
- B κάνει το εξής:
- 1)Διάβασε το input μέχρι το i-1.
- 2)Κάλεσε τον predicator A με input τα πρώτα i-1 bits.

Το unpredictability είναι ασφαλές κάτω από την υπόθεση του psedorandomness

- Υποθέτοντας ότι υπάρχει A ppt τω να μπορεί να προβλέψει το επόμενο bit με πιθανότητα ½ + κάτι μη αμελητέο, τότε μπορούμε να τον χρησιμοποιήσουμε για να διακρίνουμε αν κάτι είναι τυχαίο ή ψευδοτυχαίο με πιθανότητα μη αμελητέα.
- B κάνει το εξής:
- 1)Διάβασε το input μέχρι το i-1.
- 2)Κάλεσε τον predicator A με input τα πρώτα i-1 bits.
- 3)Υπολόγισε το επόμενο bit (το i-οστο)

Το unpredictability είναι ασφαλές κάτω από την υπόθεση του psedorandomness

- Υποθέτοντας ότι υπάρχει A ppt τω να μπορεί να προβλέψει το επόμενο bit με πιθανότητα ½ + κάτι μη αμελητέο, τότε μπορούμε να τον χρησιμοποιήσουμε για να διακρίνουμε αν κάτι είναι τυχαίο ή ψευδοτυχαίο με πιθανότητα μη αμελητέα.
- B κάνει το εξής:
- 1)Διάβασε το input μέχρι το i-1.
- 2)Κάλεσε τον predicator A με input τα πρώτα i-1 bits.
- 3)Υπολόγισε το επόμενο bit (το i-οστο)
- 4) Σύγκρινε το με το i του input,αν ταυτίζονται επέστρεψε 1, αλλιώς 0.

Πιθανότητα επιτυχίας του Β

- Η πιθανότητα επιτυχίας του Β δεδομένου ότι αυτό που πηρέ σαν input ήταν από την “σωστή” κατανομή είναι όσο και πιθανότητα επιτυχίας του Α.

Πιθανότητα επιτυχίας του B

- Η πιθανότητα επιτυχίας του B δεδομένου ότι αυτό που πηρέ σαν input ήταν από την "σωστή" κατανομή είναι όσο και πιθανότητα επιτυχίας του A.
- Ενώ η πιθανότητα να εκτυπώσει ένα δεδομένου ότι ήταν τελείως random, είναι το πολύ ½.

Πιθανότητα επιτυχίας του B

- Η πιθανότητα επιτυχίας του B δεδομένου ότι αυτό που πηρέ σαν input ήταν από την "σωστή" κατανομή είναι όσο και πιθανότητα επιτυχίας του A.
- Ενώ η πιθανότητα να εκτυπώσει ένα δεδομένου ότι ήταν τελείως random, είναι το πολύ ½.
- Άρα: $|Pr[B(G(Un))=1]-Pr[B(U_l)=1]| \geq a$

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Υποθέτουμε ότι έχουμε αλγόριθμο A τω
- $|Pr[A(G(U_n))=1]-Pr[A(U_l)=1]| \geq a$

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Υποθέτουμε ότι έχουμε αλγόριθμο A τω
- $|Pr[A(G(U_n))=1]-Pr[A(U_l)=1]| \geq a$
- Θα φτιάξουμε predicator B τω αν μας δοθούν τα πρώτα i bits να προβλέπει με πιθανότητα καλύτερη του ½ + κάτι μη αμελητέο , το επόμενο bit.

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Υποθέτουμε ότι έχουμε αλγόριθμο A τω
- $|Pr[A(G(U_n))=1]-Pr[A(U_l)=1]| \geq a$
- Θα φτιάξουμε predicator B τω αν μας δοθούν τα πρώτα i bits να προβλέπει με πιθανότητα καλύτερη του ½ + κάτι μη αμελητέο , το επόμενο bit.
- Για την απόδειξη αυτή θα χρησιμοποιηθεί το "υβριδικό επιχείρημα" (στην πιθανοτική ανάλυση).

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Η τεχνική hydrid argument ορίζει l-αδες bit,H_0,H_1,…,H_l.

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Η τεχνική hydrid argument ορίζει *l*-αδες bit, $H_0, H_1, \ldots, H_l$.
- $H_0=(z_1,z_2,\ldots,z_l)$, όπου $z_i \in_R \{0,1\}$

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Η τεχνική hydrid argument ορίζει *l*-αδες bit, $H_0, H_1, \ldots, H_l$.
- $H_0=(z_1,z_2,\ldots,z_l)$, όπου $z_i \in_R \{0,1\}$
- $H_1=(y_1,z_2,\ldots,z_l)$, όπου y_1 το πρώτο bit της γεννήτριας μας για εισοδο x (η γεννήτρια έδωσε *l* τέτοιες τιμές, από τις οποίες εμείς πήραμε την πρώτη.

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Η τεχνική hydrid argument ορίζει *l*-αδες bit, $H_0, H_1, \ldots, H_l$.
- $H_0=(z_1,z_2,\ldots,z_l)$, όπου $z_i \in_R \{0,1\}$
- $H_1=(y_1,z_2,\ldots,z_l)$, όπου y_1 το πρώτο bit της γεννήτριας μας για εισοδο x (η γεννήτρια έδωσε *l* τέτοιες τιμές, από τις οποίες εμείς πήραμε την πρώτη.
- Γενικά $H_i=(y_1,y_2,\ldots,y_i,z_{i+1},\ldots,z_l)$

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Η κατασκευή του B:

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Η κατασκευή του B:
- Δέχεται σαν είσοδο τα πρώτα i bits τις τιμής G(x)
- (όπου x $\epsilon_R \{0,1\}^n$)

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Η κατασκευή του B:
- Δέχεται σαν είσοδο τα πρώτα i bits τις τιμής G(x)
- (όπου x $\epsilon_R\{0,1\}^n$)
- Δημιουργεί τον H_i και καλεί τον A με είσοδο H_i

Το psedorandomness είναι ασφαλές κάτω από την υπόθεση του unpredictability

- Η κατασκευή του B:
- Δέχεται σαν είσοδο τα πρώτα i bits τις τιμής G(x)
- (όπου $x \epsilon_R \{0,1\}^n$)
- Δημιουργεί τον H_i και καλεί τον A με είσοδο H_i
- Αν ο A εκτυπώσει 1 τότε ο B εκτυπώνει τον z_{i+1}, αλλιώς $1-z_{i+1}$.

Πιθανοτική ανάλυση Β

- Λόγω του ότι η σχέση $|Pr[A(G(U_n))=1]-Pr[A(U_l)=1]|\geq a$
- ισχύει για απείρως πολλά n. Είτε με το ευθύ θα ισχύει για απείρως πολλά είτε το αντίθετο.

Πιθανοτική ανάλυση Β

- Λόγω του ότι η σχέση $|Pr[A(G(U_n))=1]-Pr[A(U_l)=1]|\geq a$
- ισχύει για απείρως πολλά n. Είτε με το ευθύ θα ισχύει για απείρως πολλά είτε το αντίθετο.
- Χ.Γ υποθέτω ότι ισχύει για το ευθύ, δηλαδή $Pr[A(G(Un))=1]-Pr[A(U_l)=1]\geq a$ (στην άλλη περίπτωση θα τροποποιήσουμε λιγάκι τα παρακάτω για να εκφράσουμε τα ιδία συμπεράσματα αλλά στην περίπτωση που η μηχανή εκτύπωνε ο,μας διευκολύνει για το φράξιμο)
- Ορίζω $p_i=Pr(A(H_i)=1)$

Πιθανοτική ανάλυση Β

- Λόγω του ότι η σχέση $|Pr[A(G(U_n))=1]-Pr[A(U_l)=1]|\geq a$
- ισχύει για απείρως πολλά n. Είτε με το ευθύ θα ισχύει για απείρως πολλά είτε το αντίθετο.
- Χ.Γ υποθέτω ότι ισχύει για το ευθύ, δηλαδή $Pr[A(G(Un))=1]-Pr[A(U_l)=1]\geq a$ (στην άλλη περίπτωση θα τροποποιήσουμε λιγάκι τα παρακάτω για να εκφράσουμε τα ιδία συμπεράσματα αλλά στην περίπτωση που η μηχανή εκτύπωνε ο,μας διευκολύνει για το φράξιμο)
- Ορίζω $p_i=Pr(A(H_i)=1)$
- Από υπόθεση $p_l-p_0\geq a$

Πιθανοτική ανάλυση Β

- Λόγω του ότι η σχέση $|Pr[A(G(U_n))=1]-Pr[A(U_l)=1]|\geq a$
- ισχύει για απείρως πολλά n. Είτε με το ευθύ θα ισχύει για απείρως πολλά είτε το αντίθετο.
- Χ.Γ υποθέτω ότι ισχύει για το ευθύ, δηλαδή $Pr[A(G(Un))=1]-Pr[A(U_l)=1]\geq a$ (στην άλλη περίπτωση θα τροποποιήσουμε λιγάκι τα παρακάτω για να εκφράσουμε τα ιδία συμπεράσματα αλλά στην περίπτωση που η μηχανή εκτύπωνε ο,μας διευκολύνει για το φράξιμο)
- Ορίζω $p_i=Pr(A(H_i)=1)$
- Από υπόθεση $p_l-p_0\geq a$
- Αναπτύσσω το παραπάνω σαν τηλεσκοπική σειρά, δηλαδή
- $(p_l-p_{l-1})+(p_{l-1}-p_{l-2})+\ldots+(p_1-p_0)\geq a$

Πιθανοτική ανάλυση Β

- Το $E[p_i - p_{i-1}] \geq a/l$

Πιθανοτική ανάλυση Β

- Το $E[p_i - p_{i-1}] \geq a/l$
- Παρατηρούμε ότι τουλάχιστον 1 ζευγαράκι θα υπάρχει που $p_i - p_{i-1} \geq a/l$ (αν είχαμε κράτηση τα απόλυτα λόγω τριγωνικής ανισότητας)

Πιθανοτική ανάλυση Β

- Το $E[p_i-p_{i-1}]\geq a/l$
- Παρατηρούμε ότι τουλάχιστον 1 ζευγαράκι θα υπάρχει που $p_i-p_{i-1}\geq a/l$ (αν είχαμε κράτηση τα απόλυτα λόγω τριγωνικής ανισότητας)
- Θα δείξουμε ότι $Pr[B(1^n,y_1,y_2,..,y_{i-1})=y_i]\geq 1/2+(p_i-p_{i-1})$ για κάθε i.

Πιθανοτική ανάλυση Β

- Η πιθανότητα επιτυχίας του αλγορίθμου μας είναι
- $Pr(A_{print}=1|z_i=y_i)\cdot Pr(z_i=y_i)+Pr(A_{print}=0|z_i=1-y_i)\cdot Pr(z_i=1-y_i)$
- $½\ p_i+1/2\cdot(1-Pr(A_{print}=1|z_i=1-y_i))$

Πιθανοτική ανάλυση Β

- Η πιθανότητα επιτυχίας του αλγορίθμου μας είναι
- $Pr(A_{print}=1|z_i=y_i)\cdot Pr(z_i=y_i)+ Pr(A_{print}=0|z_i=1-y_i)\cdot Pr(z_i=1-y_i)$
- $½\ p_i+1/2\cdot(1-Pr(A_{print}=1|z_i=1-y_i))$

- Ξέρουμε ότι $p_{i-1}=1/2p_i+1/2\cdot Pr(A_{print}=1|z_i=1-y_i)$

Πιθανοτική ανάλυση Β

- Η πιθανότητα επιτυχίας του αλγορίθμου μας είναι
- $Pr(A_{print}=1|z_i=y_i)\cdot Pr(z_i=y_i)+ Pr(A_{print}=0|z_i=1-y_i)\cdot Pr(z_i=1-y_i)$
- $½\ p_i+1/2\cdot(1-Pr(A_{print}=1|z_i=1-y_i))$

- Ξέρουμε ότι $p_{i-1}=1/2p_i+1/2\cdot Pr(A_{print}=1|z_i=1-y_i)$
- Αντικαθιστώντας προκύπτει το ζητούμενο.

ZERO KNOWLEDGE

- Έχουμε δυο παίκτες A,B

ZERO KNOWLEDGE

- Έχουμε δυο παίκτες A,B
- Ο A(prover) θέλει να πείσει τον B(verifier) ότι ξέρει ένα μυστικό χωρίς βεβαία να το αποκαλύψει.

ZERO KNOWLEDGE

- Έχουμε δυο παίκτες Α,Β
- Ο Α(prover) θέλει να πείσει τον Β(verifier) ότι ξέρει ένα μυστικό χωρίς βεβαία να το αποκαλύψει.
- Ο Β κάνει μια ερώτηση στον Α(challenge) που μόνο αν γνωρίζει το μυστικό (μικρή πιθανότητα να τον ξεγελάσει) να μπορεί να απαντήσει.

ZERO KNOWLEDGE

- Έχουμε δυο παίκτες Α,Β
- Ο Α(prover) θέλει να πείσει τον Β(verifier) ότι ξέρει ένα μυστικό χωρίς βεβαία να το αποκαλύψει.
- Ο Β κάνει μια ερώτηση στον Α(challenge) που μόνο αν γνωρίζει το μυστικό (μικρή πιθανότητα να τον ξεγελάσει) να μπορεί να απαντήσει.
- Έτσι ο Α έχει πείσει τον Β (με μεγάλη πιθανότητα) ότι όντως ξέρει το μυστικό, χωρίς να το αποκαλύψει.

ZERO KNOWLEDGE

- ZK proofs: Έστω L μια γλώσσα στο NP,και M(x,y) η ντετερμινιστική πολ/κου χρόνου μηχανή Turing για την οποία αν το x ϵ L υπάρχει πολ/κου μήκους πιστοποιητικό y, τω M(x,y)=1

ZERO KNOWLEDGE

- ZK proofs: Έστω L μια γλώσσα στο NP,και M(x,y) η ντετερμινιστική πολ/κου χρόνου μηχανή Turing για την οποία αν το x ϵ L υπάρχει πολ/κου μήκους πιστοποιητικό y, τω M(x,y)=1
- Ένα ζευγάρι P,V ppt αλγόριθμοι καλούνται απόδειξη μηδενικής γνώσης για την γλωσσά L αν ικανοποιούν τα εξής:

ZERO KNOWLEDGE

- ZK proofs: Έστω L μια γλώσσα στο NP,και M(x,y) η ντετερμινιστική πολ/κου χρόνου μηχανή Turing για την οποία αν το x ϵ L υπάρχει πολ/κου μήκους πιστοποιητικό y, τω M(x,y)=1
- Ένα ζευγάρι P,V ppt αλγόριθμοι καλούνται απόδειξη μηδενικής γνώσης για την γλωσσά L αν ικανοποιούν τα εξής:
- Completeness:Αν για κάθε x ϵ L και y πιστοποιητικό γι αυτό $Pr[out_V(P(x,y),V(x)]\geq 2/3$,με άλλα λόγια αν και οι δυο είναι τίμιοι(δεν ακολουθούν κάποια στρατηγική)το verify να γίνει με πιθανότητα τουλάχιστον 2/3.

ZERO KNOWLEDGE

- ZK proofs: Έστω L μια γλώσσα στο NP,και M(x,y) η ντετερμινιστική πολ/κου χρόνου μηχανή Turing για την οποία αν το x ϵ L υπάρχει πολ/κου μήκους πιστοποιητικό y, τω M(x,y)=1
- Ένα ζευγάρι P,V ppt αλγόριθμοι καλούνται απόδειξη μηδενικής γνώσης για την γλωσσά L αν ικανοποιούν τα εξής:
- Completeness:Αν για κάθε x ϵ L και y πιστοποιητικό γι αυτό $Pr[out_V(P(x,y),V(x)]\geq 2/3$,με άλλα λόγια αν και οι δυο είναι τίμιοι(δεν ακολουθούν κάποια στρατηγική)το verify να γίνει με πιθανότητα τουλάχιστον 2/3.
- Soundness:Αν x δεν ανήκει L και για οποιαδήποτε στρατηγική P* με input y, $Pr[out_V(P^*(x,y),V(x)]\leq 1/3$, δηλαδή να είναι δύσκολο ο P* κοροϊδέψει τον V σε περίπτωση που δεν έχει αυτή την γνώση.

ZERO KNOWLEDGE

- Perfect Zero Knowledge:Για κάθε ppt V* υπάρχει ένας προσδοκώμενος ppt (average case) αλγόριθμος S* τω για κάθε x ανήκει L και y πιστοποιητικό, να ισχύει:

ZERO KNOWLEDGE

- Perfect Zero Knowledge:Για κάθε ppt V* υπάρχει ένας προσδοκώμενος ppt (average case) αλγόριθμος S* τω για κάθε x ανήκει L και y πιστοποιητικό, να ισχύει:
- $out_{V^*}(P(x,y),V^*(x)) \approx S^*(x)$

ZERO KNOWLEDGE

- Perfect Zero Knowledge:Για κάθε ppt V* υπάρχει ένας προσδοκώμενος ppt (average case) αλγόριθμος S* τω για κάθε x ανήκει L και y πιστοποιητικό, να ισχύει:
- $out_{V^*}(P(x,y),V^*(x)) \approx S^*(x)$
- Δηλαδή να είναι στατιστικά αδιαχώριστα

ZERO KNOWLEDGE

- Perfect Zero Knowledge:Για κάθε ppt V* υπάρχει ένας προσδοκώμενος ppt (average case) αλγόριθμος S* τω για κάθε x ανήκει L και y πιστοποιητικό, να ισχύει:
- $out_{V*}(P(x,y),V*(x))\approx S*(x)$
- Δηλαδή να είναι στατιστικά αδιαχώριστα
- Ο S* ονομάζεται simulator για τον V*,και προσομοιώνει το output του με τον τίμιο prover P.(real/ideal paradigm,simulator base security)

Ένα παράδειγμα ZK proof

- Public input:Ένα ζευγάρι γραφήματα G_0, G_1 με n κορυφές

Ένα παράδειγμα ZK proof

- Public input:Ένα ζευγάρι γραφήματα G_0, G_1 με n κορυφές
- Prover input:Ένα permutation π :[n]->[n], τω $G_1=\pi(G_0)$

Ένα παράδειγμα ZK proof

- Public input:Ένα ζευγάρι γραφήματα G_0, G_1 με n κορυφές
- Prover input:Ένα permutation π :[n]->[n], τω $G_1=\pi(G_0)$
- Ο P διαλέγει ένα τυχαίο permutation π_1 και στέλνει στον V το $\pi_1(G_1)$

Ένα παράδειγμα ZK proof

- Public input:Ένα ζευγάρι γραφήματα G_0, G_1 με n κορυφές
- Prover input:Ένα permutation π :[n]->[n], τω $G_1=\pi(G_0)$
- Ο P διαλέγει ένα τυχαίο permutation π_1 και στέλνει στον V το $\pi_1(G_1)$
- Ο V διαλέγει b $\epsilon_R\{0,1\}$ και το στέλνει

Ένα παράδειγμα ZK proof

- Public input:Ένα ζευγάρι γραφήματα G_0, G_1 με n κορυφές
- Prover input:Ένα permutation π :[n]->[n], τω $G_1=\pi(G_0)$
- Ο P διαλέγει ένα τυχαίο permutation π_1 και στέλνει στον V το $\pi_1(G_1)$
- Ο V διαλέγει b $\epsilon_R\{0,1\}$ και το στέλνει
- Αν το b=1 ο P στέλνει το π_1, αλλιώς το $\pi_1(\pi)$

Ένα παράδειγμα ZK proof

- Public input:Ένα ζευγάρι γραφήματα G_0, G_1 με n κορυφές
- Prover input:Ένα permutation π :[n]->[n], τω $G_1=\pi(G_0)$
- Ο P διαλέγει ένα τυχαίο permutation π_1 και στέλνει στον V το $\pi_1(G_1)$
- Ο V διαλέγει b $\epsilon_R\{0,1\}$ και το στέλνει
- Αν το b=1 ο P στέλνει το π_1, αλλιώς το $\pi_1(\pi)$
- Ο V δέχεται αν $H=\pi(G_b)$,(όπου $H= \pi_1(G_1)$)

Ένα παράδειγμα ZK proof

- Αν και οι δυο παίκτες επακολουθήσουν το πρωτόκολλο ο V θα δεχτεί με πιθανότητα 1(1>2/3-> correctness)

Ένα παράδειγμα ZK proof

- Αν και οι δυο παίκτες επακολουθήσουν το πρωτόκολλο ο V θα δεχτεί με πιθανότητα 1(1>2/3-> correctness)
- Αν τα γραφήματα είναι ισομορφικά ο V θα απορρίψει με πιθανότητα ½(αν το τρέξουμε το πρωτόκολλο πιο πολλές φορές η πιθανότητα γίνεται <1/3, soundness)

Ένα παράδειγμα ZK proof

- Τώρα για το perfect ZK

Ένα παράδειγμα ZK proof

- Τώρα για το perfect ZK
- Κατασκευάζω S* ως εξής

Ένα παράδειγμα ZK proof

- Τώρα για το perfect ZK
- Κατασκευάζω S* ως εξής
- S* διαλέγει b′ ϵ_R{0,1} και ένα τυχαιο permutation π, και στέλνει το π($G_{b'}$)
- Αν το b που θα λάβει από τον V* είναι ίσο με το b′ τότε στέλνει το π στον V* και εκτυπώνει ότι και αυτός

Ένα παράδειγμα ZK proof

- Τώρα για το perfect ZK
- Κατασκευάζω S* ως εξής
- S* διαλέγει b′ ϵ_R{0,1} και ένα τυχαιο permutation π, και στέλνει το π($G_{b'}$)
- Αν το b που θα λάβει από τον V* είναι ίσο με το b′ τότε στέλνει το π στον V* και εκτυπώνει ότι και αυτός
- (λέμε ότι η εξομοίωση ήταν επιτυχής)
- Αλλιώς ξανατρέχει το πρωτόκολλο (rewind)

Ένα παράδειγμα ZK proof

- Τώρα για το perfect ZK
- Κατασκευάζω S* ως εξής
- S* διαλέγει b′ ϵ_R{0,1} και ένα τυχαιο permutation π, και στέλνει το $\pi(G_{b'})$
- Αν το b που θα λάβει από τον V* είναι ίσο με το b′ τότε στέλνει το π στον V* και εκτυπώνει ότι και αυτός
- (λέμε ότι η εξομοίωση ήταν επιτυχής)
- Αλλιώς ξανατρέχει το πρωτόκολλο (rewind)
- Παρατηρούμε ότι η πιθανότητα επιτυχίας είναι ½,και με κ επαναλήψεις ευελπιστούμε να έχει μια επιτυχία(εχει με πιθανότητα $1-2^{-\kappa}$)

Ένα παράδειγμα ZK proof

- Σε περίπτωση επιτυχούς εξομοίωσης παρατηρούμε ότι ο V* είτε μίλαγε με τον P είτε με τον S* του ήταν το ίδιο, ήταν σαν μίλαγε μονός του! Άρα ότι πληροφορία πήρε από την συζήτηση με τον P την πήρε και μιλώντας με τον εαυτό του!(τον S*)

Ένα παράδειγμα ZK proof

- Σε περίπτωση επιτυχούς εξομοίωσης παρατηρούμε ότι ο V* είτε μίλαγε με τον P είτε με τον S* του ήταν το ίδιο, ήταν σαν μίλαγε μονός του! Άρα ότι πληροφορία πήρε από την συζήτηση με τον P την πήρε και μιλώντας με τον εαυτό του!(τον S*)
- Άρα $out_{V^*}(P(x,y),V^*(x))\approx S^*(x)$

Στρίψιμο νομίσματος μέσω τηλεφώνου και δέσμευση bit

- Έστω δυο παίκτες Α,Β που θέλουν να παράγουν ένα τυχαίο bit.

Στρίψιμο νομίσματος μέσω τηλεφώνου και δέσμευση bit

- Έστω δυο παίκτες Α,Β που θέλουν να παράγουν ένα τυχαίο bit.
- Ο Α διαλέγει b ϵ_R{0,1} το δεσμεύει μέσω μια συνάρτησης com(b),και το στέλνει στον Β.

Στρίψιμο νομίσματος μέσω τηλεφώνου και δέσμευση bit

- Έστω δυο παίκτες Α,Β που θέλουν να παράγουν ένα τυχαίο bit.
- Ο Α διαλέγει b ϵ_R{0,1} το δεσμεύει μέσω μια συνάρτησης com(b),και το στέλνει στον Β.
- Ο Β διαλέγει ένα a ϵ_R{0,1} και το στέλνει στον Α.

Στρίψιμο νομίσματος μέσω τηλεφώνου και δέσμευση bit

- Έστω δυο παίκτες Α,Β που θέλουν να παράγουν ένα τυχαίο bit.
- Ο Α διαλέγει b ϵ_R{0,1} το δεσμεύει μέσω μια συνάρτησης com(b),και το στέλνει στον Β.
- Ο Β διαλέγει ένα a ϵ_R{0,1} και το στέλνει στον Α.
- Ο Α ανοίγει την δέσμευση του στον Β

Στρίψιμο νομίσματος μέσω τηλεφώνου και δέσμευση bit

- Έστω δυο παίκτες Α,Β που θέλουν να παράγουν ένα τυχαίο bit.
- Ο Α διαλέγει b ϵ_R{0,1} το δεσμεύει μέσω μια συνάρτησης com(b),και το στέλνει στον Β.
- Ο Β διαλέγει ένα a ϵ_R{0,1} και το στέλνει στον Α.
- Ο Α ανοίγει την δέσμευση του στον Β Και οι δυο υπολογίζουν το XOR(a,b) και εκτυπώνουν