Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Εφαρμοσμενων Μαθηματικων και Φυσικων Επιστημων

Τομέας Μαθηματικών
Εργαστήριο Λογικής και Επιστήμης Υπολογιστών CoReLab

Randomness Extractors and Applications to Cryptography

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Ελένης Μπακάλη

Επιβλέπων: Ευστάθιος Ζάχος
Καθηγητής ΕΜΠ

Συνεπιβλέπων: Άγγελος Κιαγιάς
Επίκ. Καθηγητής ΕΚΠΑ

Αθήνα, Οκτώβριος 2010

Ε θνικο Μετσοβιο Πολυτεχνειο
Σχολη Εφαρμοσμενων Μαθηματικων και Φυσικων Επιστημων

Τομέας Μαθηματικών
Εργαστήριο Λογικής και Επιστήμης Υπολογιστών CoReLab

Randomness Extractors and Applications to Cryptography

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Ελένης Μπακάλη

Επιβλέπων: Ευστάθιος Ζάχος
Καθηγητής ΕΜΠ

Συνεπιβλέπων: Άγγελος Κιαγιάς
Επίκ. Καθηγητής ΕΚΠΑ

Αθήνα, Οκτώβριος 2010

.....

Ελένη Μπακάλη
Διπλωματούχος Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών Ε.Μ.Π.

Copyright © Ελένη Μπακάλη, 2010.
Με επιφύλαξη παντός δικαιώματος. All rights reserved .

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Περίληψη

Ένας exrtactor είναι μία συνάρτηση η οποία παίρνει είσοδο από μία πηγή που δεν είναι ομοιόμορφη, και το αποτέλεσμα που βγάζει ακολουθεί κατανομή πολύ κοντά στην ομοιόμορφη, με τη βοήθεια μερικών πραγματικά τυχαίων bits (seed). Αυτό αποδεικνύεται χρήσιμο στην κρυπτογραφία, όταν αυτή βασίζεται σε μυστικά που δεν είναι εντελώς τυχαία (δηλ. ομοιόμορφα), οπότε με τη βοήθεια ενός extractor τα μετατρέπουμε σε τυχαία. Ένα πρόβλημα που προκύπτει, όμως, είναι όταν ο αντίπαλος αλλάξει το seed και μάθει το αποτέλεσμα του extractor για το ίδιο μυστικό, αλλά για το seed της επιλογής του. Εάν, ακόμα και με δεδομένο αυτό, το πραγματικό αποτέλεσμα του extractor εξακολουθεί να ακολουθεί την ομοιόμορφη κατανομή, ο extractor καλείται non malleable. Αποδεικνύεται ότι υπάρχουν non malleable extractors, αλλά μέχρι τώρα δεν έχουν κατασκευαστεί. Σε αυτήν την εργασία περιγράφουμε κάποιες κατασκευές από extractors και κάποιες εφαρμογές τους στην κρυπτογραφία, και επιχειρούμε επιθέσεις σε αυτούς για να δούμε κατά πόσο είναι non malleable.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τους επιβλέποντες καθηγητές μου κ. Ζάχο και κ. Κιαγιά για τις πολύτιμες συμβουλές τους και την καθοδήγηση που μου προσέφεραν. Επίσης ευχαριστώ τον κ. Παγουρτζή, τον κ. Φωτάκη, και τα παιδιά του εργαστηρίου Γεωργία Καούρη, Αντρέα Γκόμπελ, Θανάση Λιανέα, Πάρη Κουτρή, Αντρέα Γαλάνη, Μάνο Θάνο και Ματούλα Πετρόλια για τις χρήσιμες συζητήσεις, τη βοήθεια και γενικά την υποστήριξή τους. Τέλος ευχαριστώ την οικογένειά μου και τους φίλους μου, που όπως πάντα, με βοήθησαν και με υποστήριξαν.

Ελένη Μπακάλη

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Ένας exrtactor είναι μία συνάρτηση η οποία παίρνει είσοδο από μία πηγή που δεν είναι ομοιόμορφη, και το αποτέλεσμα που βγάζει ακολουθεί κατανομή πολύ κοντά στην ομοιόμορφη.

Γενικά υποθέτουμε ότι δεν ξέρουμε την κατανομή που ακολουθεί η πηγή, αλλά μας αρκεί να έχει κάποια τυχαιότητα (εντροπία), και οι extractors που κατασκευάζουμε θέλουμε να δουλεύουν για κάθε πηγή συγκεκριμένης τυχαιότητας.

Με δυο λόγια θέλουμε ένας extractor να δουλεύει για κάθε πηγή με ελάχιστη εντροπία k, χωρίς να γνωρίζουμε την κατανομή της. Δυστυχώς αυτό δεν γίνεται. Μάλιστα για κάθε ντετερμινιστικό extractor υπάρχει μία πηγή X για την οποία το $Ext(X)$ είναι σταθερό και άρα προφανώς δεν δουλέυει.

Αντίθετα, για κάθε k-source X (δηλ.πηγή με ελάχιστη εντροπία k), υπάρχει ένας καλός extractor, και μάλιστα μία τυχαία συνάρτηση είναι *extractor* με μεγάλη πιθανότητα.

Αυτό οδηγεί στην ιδέα του seeded extractor, όπου η συνάρτηση Ext παίρνει σαν είσοδο εκτός από τα n bits της πηγής, και d επιπλέον εντελώς τυχαία bits (seed). Έτσι είναι σαν να έχουμε μία οικογένεια από συναρτήσεις (extractors) και διαλέγουμε στην τύχη μία από αυτές.

Αποδεικνύεται (με την πιθανοτική μέθοδο) ότι υπάρχει πολύ καλός extractor, που δουλέυει για κάθε πηγή με ελάχιστη εντροπία k.

Επίσης ορίζεται ο Strong Extractor, ως extractor που βγάζει στην έξοδο αυτούσια και τα τυχαία bits (seed) που χρησιμοποιεί. Αυτό είναι χρήσιμο στην κρυπτογραφία, γιατί μας επιτρέπει να δημοσιοποιήσουμε το seed. Ο εχθρός επιτρέπεται να γνωρίζει το seed, και παρ΄ όλα αυτά το αποτέλεσμα να του φαίνεται (να είναι) τυχαίο.

Μπορούμε να θεωρήσουμε τους extractors σαν συναρτήσεις κατακερματισμού, και αντίστροφα να φτιάξουμε extractors από συναρτήσεις κατακερματισμού,

αρκεί η οικογένεια των συναρτήσεων να έχει την ίδιότητα της pairwise independence. Αυτό είναι το πολύ σημαντικό Leftover Hash Lemma.

Επιπλέον μπορούμε να συνθέσουμε πολλούς extractors , δηλαδή να χρησιμοποιήσουμε το αποτέλεσμα του πρώτου σαν seed για τον δεύτερο, το αποτέλεσμα του δεύτερου σαν seed για τον τρίτο, κ.ο.κ. Φυσικά μόνο για το seed του πρώτου θα χρειαστούν πραγματικά τυχαία bits.

Μία διαφορετική ιδέα για κατασκευή extractor ήταν αυτή του Trevisan, που βασίστηκε στην Nisan Wigderson γεννήτρια ψευδοτυχαίων αριθμών. Η Nisan-Wigderson (NW) γεννήτρια ψευδοτυχαίων αριθμών χρησιμοποιεί μια boolean συνάρτηση που είναι δύσκολο να προσεγγιστεί, (δεν γίνεται να προσεγγιστεί από κύκλωμα μικρού μεγέθους), και υπολογίζει την τιμή της σε πολλά τυχαία σημεία. Τα bits που παράγει φαίνονται τυχαία σε έναν υπολογιστικά περιορισμένο αντίπαλο.

Για να διαλέξει τα τυχαία σημεία στα οποία θα υπολογίσει την τιμή της f χρειάζεται μερικά πραγματικά τυχαία bits. Για να μην είναι αυτά πολλά, χρησιμεύουν οι σχεδιασμοί.

Ο Trevisan παίρνει την NW γεννήτρια, και αντί να χρησιμοποιήσει μια δύσκολα προσεγγίσιμη συνάρτηση f, χρησιμοποιεί μία τυχαία από μία πηγή X με κάποια ελάχιστη εντροπία. Το αποτέλεσμα βγαίνει ομοιόμορφο με τη βοήθεια ενός κώδικα διόρθωσης λαθών.

Οι randomness extractors αποδεικνύονται χρήσιμοι στην κρυπτογραφία, όταν αυτή βασίζεται σε μυστικά που δεν είναι εντελώς τυχαία, δηλαδή η πηγή από την οποία προέρχονται δεν ακολουθεί την ομοιόμορφη κατανομή, αλλά έχει κάποια ελάχιστη εντροπία (k bits). Σε αυτή την περίπτωση η εντροπία εκφράζει το μέγεθος της αβεβαιότητας που έχει ένας αντίπαλος για το μυστικό W.

Το θεμελιώδες πρόβλημα της κρυπτογραφίας συμμετρικού κλειδιού είναι το εξής. Η Αλίκη και ο Βασίλης μοιράζονται ένα κοινό μυστικό W και θέλουν να επικοινωνήσουν με ασφάλεια μέσω ενός δημοσίου καναλιού, που όμως ελέγχεται από έναν ενεργό αντίπαλο (την Εύα). Η επικοινωνία τους θέλουν να είναι προσωπική και αυθεντική (να είναι σίγουροι δηλαδή ότι μιλάνε μεταξύ τους και όχι με κάποιον άλλο). Αυτό το πρόβλημα λύνεται χρησιμοποιώντας βασικά κρυπτογραφικά εργαλεία, τα οποία όμως απαιτούν το μυστικό W να είναι ομοιόμορφα κατανεμημένο.

Στην πράξη είναι γενικά δύσκολο να έχει κάποιος στη διάθεσή του εντελώς τυχαία μυστικά, γιατί είτε οι φυσικές πηγές τυχαιότητας δεν είναι είναι ομοιόμορφες, όπως π.χ. τα βιομετρικά δεδομένα ή οι συνθηματικές λέξεις, είτε ο αντίπαλος έχει κάποια παράπλευρη πληροφορία σχετική με το μυστικό. Εδώ φαίνεται η χρησιμότητα των randomness extractors, γιατί η Αλίκη και ο Βασίλη-

ς μπορούν να μοιράζονται ένα τέτοιο ασθενές μυστικό W, και χρησιμοποιώντας έναν extractor να το μετατρέψουν σε ένα άλλο R ομοιόμορφα κατανεμημένο. Η μόνη απάιτηση για να μπορεί να γίνει αυτό, είναι το αρχικό μυστικό W να έχει τουλάχιστον k bits εντροπίας.

Επιπλέον, όμως, παρουσιάζεται το εξής πρόβλημα. Ο extractor που χρησιμοποιείται, χρησιμοποιεί ένα τυχαίο seed y, το οποίο γίνεται δημοσίως γνωστό και άρα γνωστό και στην Εύα. Εάν ο extractor είναι strong, τότε το αποτέλεσμα του extractor $R = Ext(W, y)$ είναι ομοιόμορφα κατανεμημένο, ακόμα και αν το seed είναι γνωστό. Τι γίνεται, όμως, αν η Εύα βλέποντας το seed y το αλλάξει σε y' της επιλογής της, και καταφέρει να μάθει το αποτέλεσμα του extractor για αυτό το seed, δηλ. το $R' = Ext(W, y')$. Θα θέλαμε, για κάθε επιλογή y' της Εύας, τα R και R' να μην σχετίζονται καθόλου. Εάν ο extractor έχει αυτήν την ιδιότητα, τότε τον καλούμε non-malleable extractor.

Αποδεικνύεται ότι τέτοιοι extractors υπάρχουν. Η απόδειξη όμως χρησιμοποιεί την πιθανοτική μέθοδο, και δεν είναι κατασκευαστική. Μέχρι τώρα δεν έχουμε explicit κατασκευή ενός non-malleable extractor.Μια ασθενέστερη έννοια που θα μπορούσαμε να ορίσουμε είναι αυτή του weak-non-malleable extractor, και ίσως να είναι ευκολότερο να βρούμε μία συνάρτηση με αυτήν την ιδιότητα. Weak non-malleable ορίζουμε να λέγεται ένας extractor αν για κάθε επιλογή y' του αντιπάλου, το R δεδομένου του R' έχει ακόμα κάποια ελάχιστη εντροπία (αν και μικρότερη από αυτήν που θα είχε αν ήταν non malleable).

Σε αυτήν την εργασία δίνουμε πρώτα τις βασικές μαθηματικές έννοιες και θεωρήματα που χρειάζονται για τη συνέχεια, ορίζουμε τους extractors και δίνουμε θεωρήματα ύπαρξης. Στο κεφάλαιο 3 περιγράφουμε μερικές κατασκευές από extractors που βασίζονται σε συναρτήσεις κατακερματισμού. Το κεφάλαιο 4 περιλαμβάνει τον extractor του Trevisan που βασίζεται σε γεννήτριες ψευδοτυχαίων αριθμών. Στο τελευταίο κεφάλαιο υπάρχουν κάποιες εφαρμογές των extractors στην κρυπτογραφία. Στο τέλος της εργασίας επιχειρούμε επιθέσεις σε γνωστούς extractors, για να δούμε κατά πόσο είναι non malleable ή weak non malleable.

Κεφάλαιο 2

Βασικές έννοιες

Σε αυτό το κεφάλαιο θα δώσουμε μερικούς ορισμούς των εννοιών με τις οποίες θα ασχοληθούμε, καθώς και βασικές ιδιότητες αυτών.

Αν θέλουμε να δούμε διαισθητικά τι είναι και τι κάνει ένας extractor , είναι μία συνάρτηση που παίρνει κάτι όχι εντελώς τυχαίο και το μετατρέπει σε τυχαίο. Για παράδειγμα θα μπορούσε ένα χαλασμένο ζάρι να το μετατρέψει σε τέλειο νόμισμα: π.χ. αν το ζάρι φέρνει τις μισές φορές 3 και τις υπόλοιπες 1,2,4,5,6 με ίσες πιθανότητες. Ένας extractor θα ήταν η συνάρτηση που αντιστοιχεί στο 3 κορώνα και στα υπόλοιπα γράμματα. Αυτό προφανώς είναι ένα τέλειο ζάρι.

Γενικά όμως θα θέλαμε ένας extractor να δουλεύει για κάθε πηγή (ζάρι) που έχει κάποια, όχι τέλεια, τυχαιότητα, χωρίς εμείς να γνωρίζουμε την ακριβή κατανομή της πηγής.

Έτσι ένας exrtactor είναι μία συνάρτηση η οποία παίρνει είσοδο από μία πηγή που δεν είναι ομοιόμορφη, και το αποτέλεσμα που βγάζει ακολουθεί κατανομή πολύ κοντά στην ομοιόμορφη.

Οπότε πρέπει να ορίσουμε τι θα πει 'κοντά', δηλαδή νά ορίσουμε κάποια απόσταση μεταξύ κατανομών. Επίσης πρέπει να ορίσουμε το πώς μετράμε την τυχαιότητα.

Παρακάτω θα δώσουμε τους αυστηρούς ορισμούς για όλα αυτά.

2.1 Κατανομές πιθανότητας

Ορισμός 1 *Μία κατανομή πιθανότητας X πάνω σε έναν (πεπερασμένο) χώρο A είναι μία συνάρτηση που αντιστοιχεί σε κάθε $a \in A$ έναν μη αρνητικό ακέραιο*

τ.ω. $0 \leq X(a) \leq 1,\ \forall a \in A$ *και* $\sum_{a \in U} X(a) = 1$.
Για ένα υποσύνολο $S \subset A$ *θα συμβολίζουμε* $X(S) = \sum_{a \in S} X(a)$.
Η ομοιόμορφη κατανομή πάνω στο A *ορίζεται* $U(a) = \frac{1}{|A|}$ *για κάθε* $a \in A$.

Θα συμβολίζουμε με το ίδιο γράμμα (π.χ. X) μία τυχαία μεταβλητή, και την κατανομή την οποία ακολουθεί η τυχαία μεταβλητή.

2.1.1 Στατιστική απόσταση

Χρειαζόμαστε μία μετρική για να μετράμε την απόσταση δύο κατανομών, και να ορίσουμε πότε δύο κατανομές είναι ¨κοντά¨.

Δύο μετρικές που χρησιμοποιούνται σε χώρους συναρτήσεων είναι οι l_1 και l_2 απόσταση, όπου

$$l_2(X, Y) = \|X - Y\| = (\sum_{a \in A} |X(a) - Y(a)|^2)^{\frac{1}{2}}$$

η ευκλείδια απόσταση, και

$$l_1(X, Y) = \sum_{a \in A} |X(a) - Y(a)|$$

η απόσταση manhattan.

Πιο σύνηθες μέτρο απόστασης για κατανομές πιθανότητας είναι η στατιστική απόσταση.

Ορισμός 2 *Έστω δύο τυχαίες μεταβλητές* X *και* Y *που παίρνουν τιμές στο* A. *Η στατιστική τους απόσταση ορίζεται*

$$\Delta(X, Y) = \max_{T \subseteq A} | \Pr[X \in T] - \Pr[Y \in T] |$$

Λέμε ότι οι X *και* Y *είναι* ϵ*-κοντά αν* $\Delta(X, Y) \leq \epsilon$, *και θα το συμβολίζουμε* $X \sim_\epsilon Y$.

Διαισθητικά, κάθε ενδεχόμενο συμβαίνει στην X και στην Y με περίπου ίση πιθανότητα.

Η στατιστική απόσταση είναι μετρική και ικανοποιεί τις εξής ιδιότητες.

1. $0 \leq \Delta(X, Y) \leq 1$, ισότητα με το μηδέν έχουμε όταν η κατανομή των X και Y είναι η ίδια, και ισότητα με τη μονάδα έχουμε όταν οι δύο κατανομές έχουν ξένα support (το support μιας συνάρτησης είναι το υποσύνολο του πεδίου ορισμού της στο οποίο είναι μη μηδενική).

2. Η $\Delta(X,Y)$ είναι συμμετρική.

3. $\Delta(X,Y) \leq \Delta(X,Z) + \Delta(Z,Y)$.

4. Για κάθε συνάρτηση f έχουμε $\Delta(f(X), f(Y)) \leq \Delta(X,Y)$.

5. $\Delta((X_1,X_2),(Y_1,Y_2)) \leq \Delta(X_1,Y_1)+\Delta(X_2,Y_2)$, αν οι X_1, X_2 είναι ανεξάρτητες, όπως επίσης και οι Y_1, Y_2.

6. $\Delta(X,Y) = \frac{1}{2} \mid X - Y \mid_1$, όπου $\mid \cdot \mid_1$ είναι η l_1 απόσταση.

Θα αποδείξουμε μόνο την ιδιότητα 6.

ΑΠΟΔΕΙΞΗ. Έχουμε $\frac{1}{2} \mid X - Y \mid_1 = \frac{1}{2} \sum_{a \in A} |X(a) - Y(a)|$, και

$$\begin{aligned} \Delta(X,Y) = \max_{T \subseteq A} \mid \Pr[X \in T] - \Pr[Y \in T] \mid = \\ \max_{T \subseteq A} \mid \sum_{a \in T} X(a) - \sum_{a \in T} Y(a) \mid = \\ \max_{T \subseteq A} \mid \sum_{a \in T} (X(a) - Y(a)) \mid \end{aligned}$$

Οπότε πρέπει να δείξουμε ότι

$$\frac{1}{2} \sum_{a \in A} |X(a) - Y(a)| = \max_{T \subseteq A} \mid \sum_{a \in T} (X(a) - Y(a)) \mid$$

Έστω $T_0 \subseteq A$ το υποσύνολο για το οποίο

$$\max_{T \subseteq A} \mid \sum_{a \in T} (X(a) - Y(a)) \mid = \mid \sum_{a \in T_0} (X(a) - Y(a)) \mid$$

Για να έχουμε max πρέπει προφανώς όλα τα $(X(a) - Y(a)),\ a \in T_0$ να είναι ομόσημα (αλλιώς κάποια θα αλληλοαναιρούνταν). Έστω, χωρίς βλάβη της γενικότητας, ότι $X(a) \geq Y(a),\ \forall a \in T_0$, οπότε

$$\mid \sum_{a \in T_0} (X(a) - Y(a)) \mid = \sum_{a \in T_0} (X(a) - Y(a))$$

Επίσης προφανώς το T_0 θα πρέπει να περιέχει όλα τα a για τα οποία $X(a) \geq Y(a)$ (αλλιώς αν υπήρχε κάποιο $a_k \in A$ με $X(a_k) \geq Y(a_k)$ και $a_k \notin T_0$, το $\sum_{a \in T_0} (X(a) - Y(a))$ δεν θα ήταν μέγιστο, αφού θα μπορούσε να αυξηθεί προσθέτωντας το a_k στο T_0).

Επομένως το T_0 είναι (χωρίς βλάβη της γενικότητας) αυτό για το οποίο ισχύει $X(a) \geq Y(a),\ \forall a \in T_0$ και $X(a) < Y(a),\ \forall a \notin T_0$. Άρα έχουμε από τη μία

$$\begin{aligned}\max_{T \subseteq A} |\sum_{a \in T}(X(a) - Y(a))| = \\ |\sum_{a \in T_0}(X(a) - Y(a))| = \\ \sum_{a \in T_0}(X(a) - Y(a))\end{aligned}$$

και από την άλλη έχουμε

$$\begin{aligned}\frac{1}{2}\sum_{a \in A}|X(a) - Y(a)| = \\ \frac{1}{2}(\sum_{a \in T_0}|X(a) - Y(a)| + \sum_{a \notin T_0}|X(a) - Y(a)|) = \\ \frac{1}{2}(\sum_{a \in T_0}(X(a) - Y(a)) + \sum_{a \notin T_0}(Y(a) - X(a))) = \\ \frac{1}{2}(\sum_{a \in T_0}(X(a) - Y(a)) + \sum_{a \notin T_0}Y(a) - \sum_{a \notin T_0}X(a)) = \\ \frac{1}{2}(\sum_{a \in T_0}(X(a) - Y(a)) + (1 - \sum_{a \in T_0}Y(a)) - (1 - \sum_{a \in T_0}X(a))) = \\ \sum_{a \in T_0}(X(a) - Y(a))\end{aligned}$$

■

2.1.2 Πιθανότητα σύγκρουσης

(collision probability)
Άλλη μία χρήσιμη έννοια για δύο τυχαίες μεταβλητές είναι της πιθανότητας σύγκρουσης.

Ορισμός 3 *Έστω X_1, X_2 δύο τυχαίες μεταβλητές που ακολουθούν την ίδια κατανομή X πάνω στο A. Η πιθανότητα σύγκρουσης της X ορίζεται $CP(X) = \Pr[X_1 = X_2] = \sum_{a \in A} X(a)^2$.*

2.1.3 Ελάχιστη εντροπία

Για να εξάγουμε m bits από μία πηγή, πρέπει αυτή να έχει τουλάχιστον m bits τυχαιότητας μέσα της. Π.χ. στο παράδειγμα που είπαμε στην αρχή, το ζάρι είχε τυχαιότητα 1 bit , αφού έφερνε 3 με πιθανότητα 1/2. Άρα δεν μπορούσαμε να κάνουμε κάτι καλύτερο, δηλαδή να πάρουμε μέσω του extractor μία κατανομή ομοιόμορφη με περισσότερα από δύο αποτελέσματα (0, 1 ή κορώνα γράμματα, δηλ 1 τυχαίο bit), γιατί θα έπερεπε όλα τα δυνατά αποτελέσματα του extractor να εμφανίζονται με ίδια πιθανότητα μικρότερη του 1/2. Αλλά αυτό δεν γίνεται γιατί ό,τι και να έκανε ένας (ντετερμινιστικός) extractor θα έφερνε τις μισές φορές το ίδιο αποτέλεσμα (το αποτέλεσμα του 3).

Γενικά υποθέτουμε ότι δεν ξέρουμε την κατανομή που ακολουθεί η πηγή, αλλά μας αρκεί να ξέρουμε την τυχαιότητά της, και οι extractors που κατασκευάζουμε θέλουμε να δουλεύουν γιά κάθε πηγή συγκεκριμένης τυχαιότητας.

Επομένως χρειαζόμαστε ένα μέτρο για να μετράμε την ΄τυχαιότητα΄ μιας τυχαίας μεταβλητής.

Για αυτό το σκοπό είναι χρήσιμη η έννοια της εντροπίας. Υπάρχουν τα εξής μέτρα εντροπίας.

- Εντροπία Shanon:

$$H_{Sh}(X) = E_{x \xleftarrow{R} X}\left[\log \frac{1}{\Pr[x = X]}\right]$$

- Εντροπία Renyi:

$$H_2(X) = \log\left(\frac{1}{E_{x \xleftarrow{R} X}[\Pr[X = x]]}\right) = \log \frac{1}{CP(X)}$$

- Ελάχιστη εντροπία:

$$H_\infty(X) = \min_x \left\{\log \frac{1}{\Pr[x = X]}\right\}$$

Ιδιότητες

Και τα τρία μέτρα ικανοποιούν τις εξής ιδιότητες.

- $0 \leq H(X) \leq \log |Supp(X)|$. Οπότε $H(X) = |Supp(X)|$ αν η X είναι ομοιόμορφη στο $Supp(X)$. ($Supp(X)$ είναι το σύνολο των x για τα οποία $\Pr[x = X] \neq 0$).
- Αν οι X και Y είναι ανεξάρτητες, τότε $H((X, Y)) = H(X) + H(Y)$.
- Για κάθε ντετερμινιστική συνάρτηση f ισχύει $H(f(X)) \leq H(X)$.
- Για κάθε X ισχύει $H_\infty(X) \leq H_2(X) \leq H_{Sh}(X)$.

Παρατηρήσεις

1. Όταν η X (ως κατανομή πάνω στο $L = \{0,1\}^n$) είναι ομοιόμορφη πάνω σε ένα υποσύνολο $S \subseteq \Lambda$, τότε $H_\infty(X) = H_{Sh}(X) = \log|S|$.

2. Αν $H_\infty(X) \geq k$ τότε $\forall x \Pr[X = x] \leq \frac{1}{2^k}$, δηλαδή η πηγή X πάνω στο $\{0,1\}^n$, παρόλο που δίνει n bits , συμπεριφέρεται σαν να έχει k τυχαία bits. Παρατηρείστε ότι η X με $H_\infty(X) = k$, έχει τόση εντροπία όση και η ομοιόμορφη στο $\{0,1\}^k$, ή όση και η ομοιόμορφη πάνω σε ένα $S \subseteq \{0,1\}^n$ με $|S| = 2^k$.

3. Για να δούμε τη διαφορά μεταξύ H_{Sh} και H_∞, έστω X η εξής κατανομή πάνω στο $\{0,1\}^n$

$$X(a) = \begin{cases} \frac{1}{2} & \text{αν } a = 0^n \\ \frac{1}{2(2^n-1)} & \text{αλλιώς} \end{cases}$$

   $H_{Sh}(X) \simeq n$, ενώ $H_\infty(X) = 1$.
   Φυσικά κάθε extractor που θα χρησιμοποιούσε ένα μόνο δείγμα από την πηγή X, τις μισές φορές θα έβγαζε ίδιο αποτέλεσμα αφού $X(0^n) = \frac{1}{2}$, παρόλο που η $H_{Sh}(X)$ είναι μεγάλη. Οπότε η ελάχιστη εντροπία είναι πιο χρήσιμη για εμάς, αφού είναι ευαίσθητη στα στοιχεία που έχουν μεγάλη πιθανότητα.
   Ο λόγος που η Shannon εντροπία χρησιμοποιείται περισσότερο στην θεωρία πληροφοριών είναι ότι εκεί συνήθως έχουμε πολλά δείγματα από την πηγή, και τότε η κατανομή (όλων των δειγμάτων μαζί) είναι κοντά στην ομοιόμορφη όπου η ελάχιστη εντροπία είναι ίση με την Shannon , και επειδή η H_{Sh} είναι πιο ευχρηστη (έχει ωραίες ιδιότητες), χρησιμοποιείται αυτή.

Η επόμενη πρόταση δίνει την ελάχιστη εντροπία μίας κατανομής που έιναι ε-κοντά στην ομοιόμορφη.

Πρόταση 1 *Έστω μία κατανομή X πάνω στο $A = \{0,1\}^m$ με $X \sim_\varepsilon U_m$. Τότε $H_\infty(X) \geq -\log(2^{-m}+\varepsilon^{-1})$. Ειδικότερα, αν $\varepsilon < \frac{1}{2^m}$ τότε $H_\infty(X) \geq m-1$, αλλιώς $H_\infty(X) \geq \log\frac{1}{\varepsilon} - 1$.*

ΑΠΟΔΕΙΞΗ. Για κάθε $a \in A$ $\Pr_{a\in A}[U_m = a] = \frac{1}{2^m}$.

$$X \sim_\varepsilon U_m \Leftrightarrow \frac{1}{2}\sum_a |X(a) - \frac{1}{2^m}| < \varepsilon \Leftrightarrow \sum_a |X(a) - \frac{1}{2^m}| < 2\varepsilon$$

Το $X(a)$ για κάθε a μπορεί να γίνει το πολύ $\frac{1}{2^m} + \varepsilon$ (και όχι 2ε γιατί πρέπει $\sum_a X(a) = 1$, οπότε αυτό που κάπου προστίθεται, αφαιρείται από κάπου

αλλού κάνοντας έτσι διπλάσιο το άθροισμα των απόλυτων διαφορών). Άρα $\max\{X(a)\} \leq \frac{1}{2^m} + \varepsilon \leq 2\max\{\frac{1}{2^m}, \varepsilon\}$. Παίρνοντας λογαρίθμους προκύπτει το ζητούμενο. ■

2.1.4 Μέση ελάχιστη εντροπία

Στην κρυπτογραφία η ελάχιστη εντροπία εκφράζει την προβλεψιμότητα ενός μυστικού W από έναν αντίπαλο. Επειδή, όμως, συνήθως ο αντίπαλος έχει κάποια πληροφορία Z σχετική με το W, πρέπει να θεωρήσουμε την προβλεψιμότητα του W δεδομένης της Z. Για αυτό το λόγο ορίζεται η μέση ελάχιστη εντροπία ως

$$H_\infty(W|Z) = -\log(E_{z\leftarrow Z} \max_w \Pr[W = w|z = Z])$$

Παρακάτω δίνονται κάποια χρήσιμα θεωρήματα που αφορούν τη μέση ελάχιστη εντροπία.

Λήμμα 1 *1. Για κάθε $\delta > 0$,*

$$\Pr_{b\leftarrow B}[H_\infty(A|B = b)] < H_\infty(A|B) - \log(\frac{1}{\delta}) \leq \delta$$

2. Αν το B παίρνει το πολύ 2^λ τιμές, τότε $H_\infty(A|(B,C)) \geq H_\infty((A,B)|C) - \lambda \geq H_\infty(A|C) - \lambda$

Ειδικότερα $H_\infty(A|B) \geq H_\infty((A,B)) - \lambda \geq H_\infty(A) - \lambda$

ΑΠΟΔΕΙΞΗ.

1. Έστω $p = (\frac{1}{2})^{H_\infty(A|B)} = E_b[2^{-H_\infty(A|B=b)}]$, $p > 0$ και άρα από την ανισότητα Markov παίρνουμε $2^{-H_\infty(A|B=b)} \leq p/\delta$ με πιθανότητα τουλάχιστον $1 - \delta$. Παίρνοντας λογαρίθμους πτοκύπτει το ζητούμενο.

2. Κατ' αρχάς η ειδική περίπτωση προκύπτει από την γενική.

   Στη γενική περίπτωση , η δεύτερη ανισότητα προκύπτει από το γεγονός ότι $\forall c \Pr[A = a \wedge B = b|C = c] \leq \Pr[A = a|C = c]$. Η πρώτη ανισότητα

αποδεικνύεται ως εξής.

$$\begin{aligned}
H_\infty(A|(B,C)) = \\
-\log E_{(b,c)\leftarrow(B,C)}\left[\max_a \Pr[A=a|B=b\wedge C=c]\right] = \\
-\log \sum_{(b,c)} \max_a \Pr[A=a|B=b\wedge C=c]\Pr[B=b\wedge C=c] = \\
-\log \sum_{(b,c)} \max_a \Pr[A=a\wedge B=b|C=c]\Pr[C=c] = \\
-\log \sum_{b} E_{c\leftarrow C}\left[\max_a \Pr[A=a\wedge B=b|C=c]\right] \geq \\
-\log \sum_{b} E_{c\leftarrow C}\left[\max_{a,b'} \Pr[A=a\wedge B=b'|C=c]\right] = \\
-\log \sum_{b} 2^{-H_\infty((A,B)|C)} \geq \\
-\log 2^{\lambda} 2^{-H_\infty((A,B)|C)} = \\
H_\infty((A,B)|C) - \lambda.
\end{aligned}$$

Η πρώτη ανισότητα ισχύει επειδή το μέγιστο για όλα τα ζεύγη (a,b') είναι μεγαλύτερο ή ίσο από το μέγιστο για όλα τα ζεύγη (a,b) με το b σταθερό.

■

2.1.5 k-sources

Ορισμός 4 *Η X είναι k-source αν $H_\infty(X) \geq k$, δηλ. $\Pr[X=x] \leq 2^{-k}$ για κάθε x.*

Ενδιαφέρουσες τιμές του k είναι κυρίως οι εξής: $k = n - O(1)$, $k = \delta n$ για σταθερά $\delta \in (0,1)$, $k = n^\gamma$ για σταθερά $\gamma \in (0,1)$, $k = polylog(n)$.

Παραδείγματα από k-sources

- Oblivious bit fixing sources: k τυχαία και ανεξάρτητα bits μαζί με $n-k$ σταθερά bits .
- Adaptive bit fixing sources: k τυχαία και ανεξάρτητα bits, και $n-k$ bits που εξαρτώνται με οποιονδήποτε τρόπο από τα πρώτα k bits .
- Santha-Vazirani δ sources:για κάθε i, κάθε $x_1,...,x_n \in \{0,1\}$ και μια σταθερά $\delta > 0$ ικανοποιούν

$$\delta \leq \Pr[X_i = 1 \mid X_1 = x_1, X_2 = x_2, ..., X_{i-1} = x_{i-1}] \leq 1-\delta$$

Μπορούμε να πάρουμε πχ $k = \log \frac{1}{(1-\delta)^n} = \Theta(\delta n)$.

- Flat k-sources: Η ομοιόμορφη κατανομή πάνω σε ένα $S \subset \{0,1\}^n$ με $|S| = 2^k$.

Οι flat k-sources είναι πολύ αντιπροσωπευτικές των k-sources για τους extractors . Αν ένας extractor δουλεύει σωστά με flat k-sources τότε δουλεύει σωστά και για κάθε k-source . Ο λόγος που συμβαίνει αυτό είναι ότι κάθε k-source είναι κυρτός συνδιασμός από flat k-sources . Οπότε μπορούμε να θεωρήσουμε ότι όταν παίρνουμε ένα δείγμα από μία k-source που είναι κυρτός συνδιασμός κάποιων flat k-sources X_i, είναι σαν να διαλέγω μία X_i (με πιθανότητα που καθορίζει ο συντελεστής της X_i στην έκφραση του κυρτού συδιασμού), και μετά να διαλέγω ένα δείγμα από την X_i.

Πρόταση 2 *Κάθε k-source είναι κυρτός συνδιασμός από flat k- sources, δηλ.* $X = \sum p_i X_i$ *με* $0 \leq p_i \leq 1$, $\sum p_i = 1$ *και όλα τα* X_i *είναι flat k-sources.*

ΑΠΟΔΕΙΞΗ. (σκαρίφημα) Μπορούμε να θεωρήσουμε κάθε πηγή X πάνω στο $[N] = 1, ..., N$ σαν ένα διάνυσμα X του $\mathbb{R}^N$, όπου κάθε συντεταγμένη $X(i),\ i = 1, ..., N$ είναι η πιθανότητα που δίνει η X στο i. Οπότε για να είναι η X κατανομή πιθανότητας, πρέπει $\forall i\ X(i) \in [0,1]$ και $\sum X(i) = 1$ (1).
Για να είναι η X k-source , πρέπει $\forall i\ X(i) \leq 2^{-k}$ (2).
Η πρώτη συνθήκη καθορίζει το υπερεπίπεδο $\sum X(i) = 1$, ενώ η δεύτερη καθορίζει τον υπερκύβο $[0, \frac{1}{2}^k]^N$. Η τομή τους είναι ένα κυρτό πολύτοπο.
Οι k-sources είναι όλα τα διανύσματα που βρίσκονται στην τομή αυτή, άρα είναι κυρτός συνδιασμών των κορυφών του πολυτόπου.
Προκύπτει ότι οι κορυφές του πολυτόπου είναι οι κορυφές του υπερκύβου για τις οποίες $X(i) = 2^{-k}$ για 2^k από τις N συντεταγμένες, και 0 για τις υπόλοιπες, δηλαδή είναι flat k-sources . ■

Εάν θέλουμε να αποδείξουμε ότι μια συνάρτηση $Ext(x,y)$ είναι $(k,\epsilon) - extractor$, αρκεί να το αποδείξουμε για τις flat k-sources.Αυτό συμβαίνει γιατί αν ο extractor αποτυγχάνει για μία οποιουδήποτε έιδους k-source , τότε υπάρχει και μία flat k-source για την οποία αποτυγχάνει.

Αυτό λέει η επόμενη πρόταση. (Δεν έχουμε ακόμα ορίσει τον extractor, αλλά για να γίνει κατανοητή η απόδειξη λέμε από τώρα ότι μια συνάρτηση $Ext(x,y) : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ είναι $(k,\epsilon) - extractor$ αν για κάθε k-source X $Ext(X, U_t) \sim_\epsilon U_m$.)

Πρόταση 3 *Εάν για μία k-source* X *ισχύει* $\Delta(Ext(X, U_t), U_m) > \epsilon$ *τότε υπάρχει μία flat k-source* X_i *για την οποία επίσης* $\Delta(Ext(X_i, U_t), U_m) > \epsilon$.

ΑΠΟΔΕΙΞΗ. Για να είναι $\Delta(Ext(X,U_t),U_m) \leq \epsilon$ αρκεί για κάθε $T : \{0,1\}^m \to \{0,1\}$ να ισχύει

$$\Pr[T(R(X,U_t)) = 1] - \Pr[T(U_m) = 1] \leq \epsilon.$$

Για να είναι $\Delta(Ext(X,U_t),U_m) > \epsilon$ πρέπει να υπάρχει T τ.ω.

$$\Pr[T(R(X,U_t)) = 1] - \Pr[T(U_m) = 1] > \epsilon \quad (1).$$

Έστω μία τιμή $x \in X$. Ορίζουμε

$$A(x) = \Pr[T(R(x,U_t)) = 1] - \Pr[T(U_m) = 1]$$

και τότε

$$\Pr[T(R(X,U_t)) = 1] - \Pr[T(U_m) = 1] = E_{x\in X}[A(x)] = E[A(X)],$$

και η (1) γράφεται $E[A(X)] > \epsilon$. (2)

Από τη πρόταση 2 έχουμε ότι η X γράφεται $X = \sum p_i X_i$ με $p_i \in [0,1]$, $\sum p_i = 1$ και X_i flat k-sources.

Η (2) γράφεται

$$E[A(X)] =$$

$$= \sum_{x\in X} \{\Pr[X = x] \cdot A(x)\}$$

$$= \sum_{x\in X} \{A(x) \cdot \underbrace{(\sum_i p_i \cdot \Pr[X_i = x])}_{\Pr[X=x]}\}$$

$$= \sum_i \{p_i (\sum_{x\in X} A(x) \cdot \Pr[X_i = x])\}$$

$$= \sum_i \{p_i (\sum_{x\in X_i} A(x) \cdot \Pr[X_i = x])\}$$

$$= \sum_i \{p_i (E[A(X_i)])\} > \epsilon \quad (3)$$

Και επειδή $\sum p_i = 1$, $p_i \in [0,1]$, για να ισχύει η (3) πρέπει να υπάρχει i τ.ω. $E[A(X_i)] > \epsilon$, δηλαδή να υπάρχει flat k-source X_i τ.ω. $\Delta(Ext(X_i,U_t),U_m) > \epsilon$. ■

2.2 Randomness Extractors

Οι randomness extractors ονομάζονται έτσι γιατί εξάγουν (extract) την τυχαιότητα που υπάρχει μέσα σε μία πηγή X. Παίρνουν δηλαδή n bits από μία πηγή X που έχει ελάχιστη εντροπία $k \leq n$, και βγάζουν m bits σχεδόν τελείως τυχαία. Φυσικά $m \leq k$ και όσο πιο κοντά είναι το m στο k τόσο καλύτερος είναι ο extractor .

Ορισμός 5 *(ντετερμινιστικός extractor) Ένας $(k, \varepsilon) - extractor$ είναι μία συνάρτηση $Ext : \{0,1\}^n \to \{0,1\}^m$ τ.ω. για κάθε πηγή με $H_\infty(X) = k$, το $Ext(X)$ είναι ϵ-κοντά στην ομοιόμορφη, δηλ. $Ext(X) \sim_\varepsilon U_m$.*

Θέλουμε ένας extractor να δουλεύει για κάθε πηγή με ελάχιστη εντροπία k, χωρίς να γνωρίζουμε την κατανομή της. Δυστυχώς αυτό δεν γίνεται και μάλιστα για κάθε ντετερμινιστικό extractor υπάρχει μία πηγή X για την οποία $Ext(X)$ =σταθερό και άρα προφανώς δεν δουλέυει.

Πρόταση 4 *Για κάθε $Ext : \{0,1\}^n \to \{0,1\}^m$ υπάρχει (n-m)-source X τ.ω. $Ext(X)$ =σταθ.*

ΑΠΟΔΕΙΞΗ. Υπάρχει $s \in \{0,1\}^m$ τ.ω. $|Ext^{-1}(s)| \geq \frac{2^n}{2^m} = 2^{n-m}$ (αρχή περιστεριώνα). Θέτουμε X να είναι η ομοιόμορφη στο $Ext^{-1}(s)$. ■

Αντίθετα, για κάθε k-source X, υπάρχει ένας καλός extractor , και μάλιστα $\forall n \in \mathbb{N}$, $\varepsilon > 0$ μία τυχαία συνάρτηση $Ext : \{0,1\}^n \to \{0,1\}^m$ είναι $(k, \varepsilon) - extractor$ με μεγάλη πιθανότητα, και $m \simeq k$.

Πρόταση 5 *Για κάθε $n, k \in \mathbb{N}$, $\varepsilon > 0$, και κάθε flat k-source X , αν διαλέξουμε μία τυχαία συνάρτηση $Ext : \{0,1\}^n \to \{0,1\}^m$ με $m = k - 2\log(1/\varepsilon) - O(1)$, τότε $Ext(X) \sim_\varepsilon U_m$ με πιθανότητα $1 - 2^{M - \Omega(K\varepsilon^2)}$, όπου $K = 2^k, M = 2^m$.*

ΑΠΟΔΕΙΞΗ. Έστω flat k-source X.

Έστω R τυχαία μεταβλητή ομοιόμορφα κατανεμημένη στο χώρο των συναρτήσεων $R : \{0,1\}^n \to \{0,1\}^m$.

Θέλουμε για κάθε $T : \{0,1\}^m \to \{0,1\}$, $|\Pr_{x \in X}[T(R(x)) = 1] - \Pr[T(U_m) = 1]| \leq \varepsilon$. (1)

Φιξάρουμε το T.

Ορίζουμε $p(R) = \Pr_{x \in X}[T(R(x)) = 1] - \Pr[T(U_m) = 1]$.

Έστω η τ.μ. $Q(x) = T(R(x)) - E[T(U_m)]$.

Τότε $p(R) = \bar{Q} = \frac{\sum_x Q(x)}{2^k}$.

Θέλω να φράξω την $\Pr_R[|p(R)| > \varepsilon]$. Επειδή η R είναι τυχαία, δηλαδή για κάθε x $R(x) \sim U_m$, έχουμε $E_R[Q(x)] = 0$ και άρα $E_R[\bar{Q}] = 0$.

Παίρνοντας Chernoff bound $\Pr_R[|p(R)| > \varepsilon] \leq 2^{-\Omega(k\varepsilon^2)}$.

Τώρα παίρνουμε ενιαίο φράγμα για όλα τα T (2^M στο πλήθος), οπότε η πιθανότητα να υπάρχει T τ.ω. η (1) να μην ισχύει (δηλ ο τυχαίος R να μην είναι extractor), είναι $2^M \cdot 2^{-\Omega(k\varepsilon^2)}$, που είναι μικρότερη από 1 αν $m = k - 2\log(1/\varepsilon) - O(1)$. ■

Αυτό οδηγεί στην ιδέα του seeded extractor , όπου η συνάρτηση Ext παίρνει σαν είσοδο εκτός από τα n bitsτης πηγής, και d επιπλέον εντελώς τυχαία bits (seed). Έτσι είναι σαν να έχουμε μία οικογένεια από συναρτήσεις (extractors) και διαλέγουμε στην τύχη μία από αυτές.

Ορισμός 6 *(seeded extractor)Ενας $(k, \varepsilon) - extractor$ είναι μία συνάρτηση $Ext : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ τ.ω. για κάθε k-source X το $Ext(X, U_d)$ είναι ϵ-κοντά στην U_m.*

Στο εξής, όταν λέμε extractor θα εννοούμε seeded extractor .

Αποδεικνύεται ότι υπάρχει πολύ καλός extractor , που δουλέυει για κάθε πηγή με ελάχιστη εντροπία k. Πολύ καλός εννοούμε από την άποψη ότι το d είναι πολύ μικρό (λογαριθμικό σε σχέση με το n), και $m \simeq k+d$, δηλαδή βγάζει όλη την τυχαιότητα που υπάρχει στην πηγή και στο seed μαζί.

Θεώρημα 7 *Για κάθε $n, k \leq n, \varepsilon > 0$ υπάρχει ένας $(k, \varepsilon) - extractor$ $Ext : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ με $m \leq k + d - 2\log(\frac{1}{\varepsilon}) - O(1)$ αν $d \geq \log(n - k) + 2\log(\frac{1}{\varepsilon}) + O(1) + m - k$.*

ΑΠΟΔΕΙΞΗ. Η απόδειξη γίνεται με την πιθανοτική μέθοδο. Αρκεί ο extractor να λειτουργεί για τις flat k-sources. Διαλέγουμε τον ectractor Ext στην τύχη. Τότε η πιθανότητα να αποτύχει είναι το πολύ ίση με το πλήθος των flat k-sources επί την πιθανότητα να αποτύχει για μία συγκεκριμένη flat k-source. Από την προηγούμενη πρόταση, η πιθανότητα αποτυχίας για μια συγκεκριμένη flat k-source είναι το πολύ $2^{M-\Omega(KD\varepsilon^2)}$, αφού η (X, U_d) είναι flat (k+d)-source, και $m \leq k + d - 2\log(\frac{1}{\varepsilon}) - O(1)$. Άρα η συνολική πιθανότητα αποτυχίας είναι

$$\binom{N}{K} \cdot 2^{M-\Omega(KD\varepsilon^2)} \leq (\frac{Ne}{K})^K 2^{M-\Omega(KD\varepsilon^2)}.$$

Η τελευταία έκφραση είναι μικρότερη της μονάδας αν $D\varepsilon^2 \geq \log\frac{Ne}{K} + \frac{M}{K} = c(n-k) + c' + \frac{M}{K}$ για σταθερές c, c'. Αυτό είναι ισοδύναμο με $d \geq \log(n-k) + 2\log(frac1\varepsilon) + O(1) + m - k$. ■

Πόρισμα 1 *Για κάθε* $n, k \leq n, \varepsilon > 0$ *υπάρχει* (k,ε)*-extractor* $Ext : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$ *με* $m = k$, *αν* $d \geq \log(n-k) + 2\log(\frac{1}{\varepsilon}) + O(1) = O(\log(n/\varepsilon))$.

Και τώρα θα δώσουμε τον ορισμό του Strong Extractor , που είναι χρήσιμος στην κρυπτογραφία, γιατί μας επιτρέπει να δημοσιοποιήσουμε το seed.

Ορισμός 8 *(Strong Extractor)Μία συνάρτηση* $Ext : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$ *είναι strong* $(k,\varepsilon) - extractor$, *αν για κάθε k-source πάνω στο* $\{0,1\}^n$, $(U_d, Ext(X,U_d)) \sim_\varepsilon (U_d, U_m)$. *Ισοδύναμα,* $Ext'(x,y) = (y, Ext(x,y))$ *είναι απλός* $(k,\varepsilon) - extractor$.

Αποδεικνύεται επίσης όπως και πριν ότι υπάρχουν πολύ καλοί strong extractors.

Θεώρημα 9 *Για κάθε* $n, k \leq n, \varepsilon > 0$ *υπάρχει ένας strong* $(k,\varepsilon) - extractor$ $Ext : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$ *με* $m = k - 2\log(\frac{1}{\varepsilon}) - O(1)$ *και* $d = \log(n-k) + 2\log(\frac{1}{\varepsilon}) + O(1)$.

Παρατήρηση Παρατηρούμε ότι τώρα έχουμε $m \simeq k$ αντί για $m \simeq k+d$, και τα d τυχαία bits βγαίνουν αυτούσια στην έξοδο. Άρα το αποτέλεσμα $Ext(x,y)$ είναι κοντά στην ομοιόμορφη, ακόμα και αν το seed γίνεται γνωστό (βγαίνει στην έξοδο).

Αυτό για την κρυπτογραφία σημαίνει ότι ο εχθρός επιτρέπεται να γνωρίζει το seed, και παρ' όλα αυτά το αποτέλεσμα να του φαίνεται (να είναι) τυχαίο.

Εδώ, όμως, μπορεί κάποιος να έχει την εξής αντίρρηση. Αφού το seed γίνεται γνωστό, τότε ο extractor γίνεται ντετερμινιστικός, και άρα υπάρχει πηγή για την οποία δεν δουλεύει.

Πράγματι, έστω $n \in \mathbb{N}$, $\varepsilon > 0$ και $k_0 = \frac{n}{2} + \log\frac{1}{\varepsilon} + \frac{O(1)}{2}$. Από το θεώρημα 9 υπάρχει strong $(k_0,\varepsilon) - extractor$ με $m = k - 2\log(\frac{1}{\varepsilon}) - O(1)$. Οπότε $k = n - m$.
Έστω τώρα $y_0 \in \{0,1\}^d$ το (γνωστό) seed, και ο ντετερμινιστικός extractor $Ext_{y_0}(x) = Ext(x,y_0) : \{0,1\}^n \rightarrow \{0,1\}^m$. Από την πρόταση 4 υπάρχει k_0-source X_0 τ.ω. $Ext_{y_0}(X_0) =$σταθ.

Επομένως το γεγονός ότι $(U_d, Ext(X,U_d)) \sim_\varepsilon (U_d, U_m)$ δεν σημαίνει ότι ξέροντας το $y \in U_d$ ισχύει $Ext(X,U_d) \sim_{\varepsilon_1} U_m$, ότι δηλαδή ο εχθρός δεν μπορεί να μαντέψει το $Ext(x,y)$, απλώς ότι για το τυχαίο y δεν μπορεί , και ότι είναι λίγα αυτά για τα οποία μπορεί.

Επιπλέον, προφανώς, επειδή δεν ξέρει εξαρχής το y_0, δεν μπορεί να βρει και να μας δώσει από πριν την πηγή X_0.

Άρα με μεγάλη πιθανότητα, για κάθε πηγή και για κάθε seed, το αποτέλεσμα του extractor είναι τυχαίο, ακόμα και αν ο αντίπαλος γνωρίζει το seed.

Το γεγονός ότι είναι λίγα τα seeds y για τα οποία το $Ext(x,y)$ δεν είναι ομοιόμορφο προκύπτει από το εξής.

$$(Y, Ext(X,Y)) \sim_\varepsilon (U_d, U_m) \Leftrightarrow$$

$$\forall T : \{0,1\}^n \times \{0,1\}^d \to \{0,1\} \mid \Pr_{y,x}[T(y, Ext(x,y)) = 1] - \Pr[T(U_d, U_m) = 1]| \leq \varepsilon$$

Έστω T (αντίπαλος). Χωρίς βλάβη της γενικότητας βγάζουμε την απόλυτη τιμή.

$$\Pr_{y,x}[T(y, Ext(x,y)) = 1] - \Pr[T(U_d, U_m) = 1] \leq \varepsilon \Leftrightarrow$$

$$E_{y,x,r}[T(y, Ext(x,y)) - T(y,r)] \leq \varepsilon \ (1)$$

όπου $r \sim U_m,\ y \sim U_d,\ x \sim X$. Έστω B το σύνολο των $y \in \{0,1\}^d$ για τα οποία $f(y) \equiv E_{x,r}[T(y, Ext(x,y) - T(y,r))] > \varepsilon$, οπότε έχω

$$(1) \Leftrightarrow E_{y \in B}[f(y)]\dot{\Pr}[Y \in B] + E_{y \notin B}[f(y)]\dot{\Pr}[Y \notin B] \leq \varepsilon$$

$$E_{y \in B}[f(y)]\dot{\Pr}[Y \in B] \leq \varepsilon$$

Οπότε όσο μεγαλώνει το $E_{y \in B}[f(y)]$, δηλαδή η πιθανότητα ο T να ξεχωρίσει το $Ext(x,y)$ από το τυχαίο, τόσο μικραίνει το $\Pr[Y \in B]$, δηλαδή το πλήθος των y για τα οποία μπορεί να το κάνει αυτό (έτσι ώστε το γινόμενό τους να παραμένει $\leq \varepsilon$).

Πιο συγκεκριμένα , από το λήμμα 1 έχουμε ότι για κάθε $\delta > 0$, για ένα ποσοστό $1 - \delta$ των y (δηλαδή για τα περισσότερα)

$$H_\infty(R|Y = y) > H_\infty(R|Y) - \log(1/\delta) > H_\infty((R,Y)) - d - \log(1/\delta)$$

όπου $R = Ext(X,Y)$.

Οπότε αν $(R,Y) \sim_\varepsilon U_{m+d}$ τότε $H_\infty((R,Y)) \simeq m + d$ (αν το ε είναι πολύ μικρό) και τότε $H_\infty(R|Y = y) > m - \log(1/\delta)$ για τα περισσότερα y.

Αναφορές. Η ελάχιστη εντροπία ορίζεται στο [1]. Η μέση ελάχιστη εντροπία και τα δύο σχετικά θεωρήματα στο [2]. Οι k-sources στα [20],[21]. Οι extractors στο [11] και τα θεωρήματα ύπαρξης και μη ύπαρξης στα [14, 13, 15].

Κεφάλαιο 3

Extractors από συναρτήσεις κατακερματισμού

Μπορούμε να θεωρήσουμε τους extractors σαν συναρτήσεις κατακερματισμού, και αντίστροφα να φτιάξουμε extractors από συναρτήσεις κατακερματισμού.

Είχαμε αποδείξει ότι για κάθε flat k-source , μια τυχαία συνάρτηση $h : \{0,1\}^n \to \{0,1\}^m$ για $m < k$, είναι extractor με μεγάλη πιθανότητα, που σημαίνει ότι αν το H είναι ομοιόμορφα κατανεμημένο πάνω σε όλες τις συναρτήσεις $h : \{0,1\}^n \to \{0,1\}^m$ και το X είναι flat k-source τότε η $(H, H(X))$ είναι στατιστικά κοντά στην (H, U_m), δηλαδή έχουμε strong extractor.

Μπορούμε αντί να χρησιμοποιήσουμε μια μικρότερη οικογένεια από συναρτήσεις κατακερματισμού, αντί για όλες (που είναι $(2^m)^{2^n}$ στο πλήθος)· Αποδεικνύεται ότι αυτό γίνεται, και μάλιστα ότι αρκεί η οικογένεια να έχει την ίδιότητα της pairwise independence . Αυτό είναι το πολύ σημαντικό Leftover Hash Lemma. Τελικά το μέγεθος της οικογένειας μειώνεται σε $O(2^n)$ (που σημαίνει ότι χρειαζόμαστε $O(n)$ πραγματικά τυχαία bits στο seed του extractor.

Επιπλέον μπορούμε να μειώσουμε κι άλλο το μέγεθος του seed σε $O(\log n)$, συνθέτοντας πολλούς extractors , δηλαδή χρησιμοποιώντας το αποτέλεσμα του πρώτου σαν seed για τον δεύτερο, το αποτέλεσμα του δεύτερου σαν seed για τον τρίτο, κ.ο.κ. Φυσικά μόνο για το seed του πρώτου θα χρειαστούν πραγματικά τυχαία bits.

3.1 Leftover Hash Lemma

Οι επόμενες δύο προτάσεις είναι βοηθητικές για την απόδειξη του πολύ σημαντικού Leftover Hash Λήμματος. Το Leftover Hash Lemma αποδεικνύεται στο [5].

Πρόταση 6 *Αν μία πηγή X πάνω στο $[N]$ έχει ελάχιστη εντροπία $H_\infty(X) =$*

k *τότε* $CP(X) \leq 1/K$

ΑΠΟΔΕΙΞΗ. Επειδή $H_\infty(X) = k$ έχω $\forall x \in [N]$

$$p_x = \Pr[X = x] \leq \frac{1}{2^k} = \frac{1}{K}$$

Επίσης προφανώς $\sum_{x \in X} p_x = 1$

$$CP(X) = \sum_{x \in X} p_x^2 \leq \sum_{x \in X} p_x \cdot \frac{1}{K} = \frac{1}{K} \sum_{x \in X} p_x = \frac{1}{K}$$

■

Πρόταση 7 *Έστω* X, Y, U_L *κατανομές πάνω στο* $[L]$. *Ισχύει*

1. $\|X - U_L\|^2 \leq CP(X) - CP(U_L)$
2. $|X - Y|_1 \leq \|X - Y\|^2$

ΑΠΟΔΕΙΞΗ. Έστω για κάθε $i \in [L]$
$x_i = \Pr[X = i]$
$y_i = \Pr[Y = i]$
$u_i = \Pr[U_L = i] = \frac{1}{L}$

1.

$$CP(U_L) = \sum_{i=1}^{L} u_i^2 = \sum_{i=1}^{L} \frac{1}{L^2} = \frac{1}{L}$$

$$\|X - U_L\|^2 = \sum_{i=1}^{L} |x_i - u_i|^2 = \sum_{i=1}^{L} (x_i^2 + (\frac{1}{L})^2 - 2\frac{x_i}{L}) =$$

$$\underbrace{\sum_{i=1}^{L} x_i^2}_{=CP(X)} + \frac{1}{L} - \frac{2}{L} \underbrace{\sum_{i=1}^{L} x_i}_{=1} = CP(X) - \frac{1}{L} = CP(X) - CP(U_L)$$

2.

$$|X - Y|_1^2 = (\sum_{i=1}^{L} |x_i - y_i|)^2 \leq \sum_{i=1}^{L} |x_i - y_i|^2 = \|X - Y\|^2$$

$$\Rightarrow |X - Y|_1 \leq \|X - Y\|$$

■

Ορισμός 10 *Μια οικογένεια συναρτήσεων* $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^m\}$ *λέγεται pairwise independent αν για κάθε ζευγάρι* $x_1 \neq x_2 \in \{0,1\}^n$ *ισχύει* $Pr_h[h(x_2) = w_2 \mid h(x_1) = w_1] = \frac{1}{M} = \Pr_h[h(x_2) = w_2]$ *για κάθε* $w_1, w_2 \in \{0,1\}^m$.

Θεώρημα 11 *(Leftover Hash Lemma) Έστω* $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^m\}$ *μια οικογένεια συναρτήσεων pairwise independent όπου* $m = k - 2\log\frac{1}{\varepsilon}$, *τότε* $Ext(x,h) \stackrel{def}{=} h(x)$ *είναι strong* (k,ε) *extractor.*

ΑΠΟΔΕΙΞΗ. Έστω μια $k - source$ στο $\{0,1\}^n$ και $H \stackrel{R}{\leftarrow} \mathcal{H}$.
Έστω d το μήκος του seed, $d = \log|\mathcal{H}|$.
Πρέπει να δείξουμε ότι η $(H, H(x))$ είναι ε-κοντά στην $U_d \times U_m$, δηλαδή ότι $\Delta((H,H(X)), U_d \times U_m) \leq \varepsilon$.

$$\begin{aligned} \Delta((H,H(X)), U_d \times U_m) = \\ \frac{1}{2} \mid (H,H(X)) - U_d \times U_m \mid_1 \leq \\ \frac{1}{2}\|(H,H(X)) - U_d \times U_m\| \leq \\ \frac{1}{2}(CP(H,H(X)) - CP(U_d \times U_m))^{\frac{1}{2}} \end{aligned} \tag{3.1}$$

Μένει να υπολογίσουμε τα $CP(H,H(X))$ και $CP(U_d \times U_m)$.
$CP(U_d \times U_m) = \frac{1}{DM}$.
$CP(H,H(X)) \stackrel{def}{=} \Pr[(H,H(X)) = (H',H'(X'))]$ όπου τα (H,X) και (H',X') είναι ανεξάρτητα και ακολουθούν την ίδια κατανομή.
Βλέπουμε ότι $(H,H(X)) = (H',H'(X'))$ ανν $H = H'$ και είτε $X = X'$ είτε $X \neq X'$ αλλά $H(X) = H(X')$, δηλαδή

$$\begin{aligned} \Pr[(H,H(X)) = (H',H'(X'))] = \\ \Pr[H = H'] \cdot (\Pr[X = X'] + \Pr[H(X) = H(X') \mid X \neq X']) = \\ CP(H)(CP(X) + \Pr[H(X) = H(X') \mid X \neq X']) = \\ \frac{1}{D}(\frac{1}{K} + \frac{1}{M}) \end{aligned}$$

Αυτό γιατί η H επιλέγεται ομοιόμορφα από την $\mathcal{H}$ που έχει $|\mathcal{H}| = D$.
Επίσης η X έχει $H_\infty(X) \geq k$ άρα $CP(X) \leq \frac{1}{K}$.
Επίσης $\Pr[H(X) = H(X') \mid X \neq X'] = \frac{1}{M}$ επειδή οι h είνα pairwise indepen-

dent . Άρα $CP(H, H(X)) = \frac{K+M}{DKM} = \frac{1+\frac{M}{K}}{DM}$. Άρα

$$\Delta((H, H(X)), U_d \times U_m) \overset{3.1}{\leq}$$
$$\frac{1}{2}(CP(H, H(X)) - CP(U_d \times U_m))^{\frac{1}{2}} =$$
$$\frac{1}{2}(\frac{1+\frac{M}{K}}{DM} - \frac{1}{DM})^{\frac{1}{2}} =$$
$$\frac{1}{2}\sqrt{\frac{M/K}{DM}} \leq \sqrt{\frac{M}{K}} = \varepsilon$$

Αυτό γιατί $m = k - 2\log\frac{1}{\varepsilon} \Rightarrow M = K\varepsilon^2 \Rightarrow \varepsilon = \sqrt{\frac{M}{K}}$. ■

Σημείωση Αν είναι δεδομένα τα k και ε τότε προκύπτει ότι πρέπει $m \leq k - 2\log\frac{1}{\varepsilon}$. Αν είναι δεδομένα τα k και m τότε παίρνω $\varepsilon = \sqrt{\frac{M}{K}}$.

Σημείωση Αν έχω οικογένεια $\mathcal{H}$ με σφάλμα σύγκρουσης δ, δηλαδή $\Pr_h[h(x) = h(x') \mid x \neq x'] \leq \frac{1+\delta}{M}$, τότε παίρνω $\Delta((H, H(X)), U_d \times U_m) \leq \frac{1}{2}\sqrt{\frac{M/K+\delta}{DM}} = \varepsilon$. Οπότε αν $K = O(M/\delta)$ παίρνω $\varepsilon = O(\sqrt{\delta})$.

3.2 Υλοποίηση του Leftover Hash Λήμματος

Επομένως για να υλοποήσουμε τον extractor που δίνει το Leftover Hash Lemma, χρειαζόμαστε μία οικογένεια συναρτήσεων που να έιναι pairwise independent. Η παρακάτω οικογένεια συναρτήσεων κατακερματισμού έχει αυτήν την ιδιότητα.

Ορισμός 12 *Έστω p πρώτος και $s = (a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$. Ορίζουμε την $h_s : \mathbb{Z}_p \to \mathbb{Z}_p$ ώς $h_s(x) = (ax + b) \mod p$.*

Θεώρημα 13 *Η οικογένεια $\mathcal{H} = \{h_s(x) = ax + b \mod p \mid s = (a, b) \in [p] \times [p]\}$ είναι pairwise independent.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε όλες τις πράξεις modulo p.

Αν για κάποιο $s \in \mathbb{Z}_p^2$ έχω $h_s(x) = w_1$ και $h_s(x) = w_2$ για κάποια $w_1, w_2 \in \mathbb{Z}_p$, δηλαδή

$$ax + b = w_1 \wedge ay + b = w_2$$

υπάρχει περίπτωση και για άλλο $s' \neq s$ να συμβαίνει αυτό; δηλαδή

$$a'x + b = w_1 \wedge a'y + b = w_2$$

Αυτό θα σήμαινε

$$\left.\begin{array}{lll}(ax+b)=(a'x+b') & \mod p \overset{p\ prime}{\Rightarrow} x=(b'-b)(a-a')^{-1} & \mod p \\ (ay+b)=(a'y+b') & \mod p \overset{p\ prime}{\Rightarrow} y=(b'-b)(a-a')^{-1} & \mod p \end{array}\right\} \Rightarrow$$

$$\Rightarrow x=y \mod p$$

Άρα αν $x \neq y$ τότε για κάθε $s=(a,b)$ έχω διαφορετικό ζευγάρι $(h_s(x), h_s(y))$, συνολικά p^2 το πλήθος.

Άρα για $x \neq y$ και $w_1, w_2 \in \mathbb{Z}_p$ δεδομένα

$$\begin{aligned}\Pr[h_s(x)=w_1 \wedge h_s(y)=w_2] = \\ \Pr[(h_s,h_s)=(w_1,w_2)] = \\ \frac{1}{p^2}=\frac{1}{p}\cdot\frac{1}{p}= \\ \Pr[h_s(x)=w_1]\cdot\Pr[h_s(y)=w_2]\end{aligned}$$

(Η τελευταία ισότητα $\Pr[h_s(x)=w_1]$ ισχύει γιατί για κάθε $a \in \mathbb{Z}_p$ έχω $ax+b=w_1 \mod p$ για ακριβώς ένα b, επομένως από τα p^2 το πλήθος ζεύγη (a,b) έχω $h_s(x)=w_1$, για p το πλήθος ζεύγη. Άρα $\Pr[h_s(x)=w_1]=\frac{p}{p^2}=\frac{1}{p}$).

Άρα η οικογένεια είναι pairwise independent. ■

Σημείωση Αν θέλω οι συναρτήσεις κατακερματισμού να είναι $h_s : [N] \to [M]$ με $m < n$ τότε διαλέγαμε ένα πρώτο $p > N$ της μορφής $p = 2^\lambda - 1$, υπολογίζουμε την $h'_s(x) : \mathbb{Z}_p \to \mathbb{Z}_p$ όπως περιγράψαμε και κρατάμε τα πρώτα m bits του $h_s(x)$.
Το $p = 2^\lambda - 1$ γράφεται σε διαδική ανάπαράσταση ως $\underbrace{11...1}_{\sharp n}$ οπότε και να κρατήσω τα πρώτα m bits του $h_s(x)$, θα διατηρείται η ομοιομορφία του αποτελέσματος, αφού κάθε τιμή θα εμφανίζεται ίσες φορές (εκτός από την $\underbrace{11...1}_{\sharp m}$ που θα εμφανίζεται μία λιγότερη).

Σημείωση

1. Η παραπάνω οικογένεια είναι pairwise independent.
2. Κάθε συνάρτηση $h_s(x)$ υπολογίζεται εύκολα.
3. Απαιτούνται $2\log p = O(n)$ τυχαία bits για την επιλογή της h_s.

Σημείωση Είπαμε ότι αν $x \neq y$ τότε για κάθε $(a,b) = s$ έχω διαφορετικό $(h_s(x), h_s(y))$, που σημαίνει ότι αν διαλέξουμε το s τυχαία και ομοιόμορφα από το $[p]^2$, τότε και το $(h_s(x), h_s(y))$ κατανέμεται επίσης ομοιόμορφα στο $[p] \times [p]$. Αυτή η ιδιότητα των συναρτήσεων κατακερματισμού λέγεται 2-universal.

3.3 Σύνθεση από Extractors

Αφού ένας (srong) extractor πολλαπλασιάζει τα d τυχαία bits , παίρνοντας ένα τυχαίο string (seed)απο d bits, και βγάζοντας επιπλέον m (σχεδόν) τυχαία bits , μπορούμε να συνθέσουμε δύο extractors χρησιμοποιώντας τα (σχεδόν) τυχαία bits που βγάζει στην έξοδο ο ένας, σαν είσοδο (seed) για τον δεύτερο. Οπότε πολλαπλασιάζουμε περισσότερο τα αρχικά τυχαία bits.

Το πρόβλημα, όμως, είναι ότι για να το κάνουμε αυτό θα χρειαζόμασταν δύο πηγές, ή δύο δείγματα από μία πηγή. Υποτίθεται, όμως , ότι έχουμε στη διάθεσή μας μόνο ένα δείγμα από μία πηγή.

Αυτό, όπως θα δούμε, αντιμετωπίζεται μετατρέποντας την πηγή που έχουμε, σε block-wise source.

3.3.1 Σύνθεση από δύο extractors

Ορισμός 14 *Έστω δύο extractors* $G_1 : \{0,1\}^{n_1} \times \{0,1\}^{d_1} \to \{0,1\}^{m_1}$, $G_2 : \{0,1\}^{n_2} \times \{0,1\}^{d_2} \to \{0,1\}^{m_2}$ *με* $m_2 = d_1$. *Ορίζουμε τη σύνθεση* $G_1 \circ G_2 : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \times \{0,1\}^{d_2} \to \{0,1\}^{m_1}$ *ως* $G_1 \circ G_2 = G_1(x_1, G_2(x_2, y))$.

Το αν η κατανομή του $G_1 \circ G_2(X_1, X_2, Y)$ είναι κοντά στην ομοιόμορφη, εξαρτάται από το αν οι τυχαίες μεταβλητές X_1, X_2 είναι ανεξάρτητες. Αποδεικνύεται [1] ότι αρκεί για τις X_1, X_2 να είναι block-wise source.

Ορισμός 15 *Έστω* X_1, X_2 *δύο τυχαίες μεταβλητές που παίρνουν τιμές στα* $\{0,1\}_1^n, \{0,1\}_2^n$ *αντίστοιχα. Λέμε ότι η* (X_1, X_2) *είναι μία* (k_1, k_2) *block-wise source αν*

1. $H_\infty(X_1) \geq k_1$
2. *Για κάθε τιμή* x_1 *της* X_1, $H_\infty(X_2|X_1 = x_1) \geq k_2$

Λήμμα 2 *Έστω* $G_1 : \{0,1\}^{n_1} \times \{0,1\}^{d_1} \to \{0,1\}^{m_1}$ *ένας* (k_1, ϵ_1)*-extractor και* $G_2 : \{0,1\}^{n_2} \times \{0,1\}^{d_2} \to \{0,1\}^{m_2}$ *ένας* (k_2, ϵ_2)*-extractor. Αν* X_1, X_2 *είναι* $(k_1, k_2$ *block-wise source και το* y *τυχαίο, τότε η κατανομή του* $G_1 \circ G_2(x_1, x_2, y)$ *είναι* $(\epsilon_1 + \epsilon_2)$*-κοντά στην ομοιόμορφη.*

ΑΠΟΔΕΙΞΗ. (σκαρίφημα) Το $W = G_2(X_2, U_{d_2})$ για $X_1 = x_1$ είναι ϵ_2-κοντά στην ομοιόμορφη. Αυτό για όλα τα x_1, άρα και η από κοινού κατανομή (X_1, W) είναι ϵ_2-κοντά στην (X_1, U_d). Άρα και η $G_1(X_1, W)$ είναι ϵ_2-κοντά στην $G_1(X_1, U_{d_1})$. Αλλά η $G_1(X_1, U_{d_1})$ είναι ϵ_1 κοντά στην ομοιόμορφη, άρα η $G_1 \circ G_2 = G_1(X_1, W)$ είναι $(\epsilon_1 + \epsilon_2)$-κοντά στην ομοιόμορφη. ■

Γενίκευση για περισσότερους extractors

(Αυτή η παράγραφος είναι λίγο δυσνόητη σε πρώτη ανάγνωση, γιατί εκτός από τη γενίκευση για περισσότερους από δύο ectractors , γενικεύει και για την περίπτωση που έχουμε πηγή που δεν είναι block wise , αλλά είναι στατιστικά κοντά σε μία block wise source.

Επίσης οι ακριβείς κατασκευές δεν δίνονται, οπότε ο αναγνώστης μπορεί να αντρέξει στη βιβλιογραφία.)

Ορισμός 16 *[10] Έστω $B_1, ..., B_t$ συσχετισμένες τυχαίες μεταβλητές που παίρνουν τιμές στα $[N_1], ..., [N_t]$ αντίστοιχα. Η $(B_1, ..., B_t)$ λέγεται $(k_1, ..., k_t)$ block-wise source με σφάλμα ϵ, αν για κάθε $1 \leq i \leq t$ και για $(1 - \epsilon)$ ποσοστό των ακολουθιών $x_1, ..., x_{i-1}$, η κατανομή $(B_i | B_1 = x_1, ..., B_{i-1} = x_{i-1})$ είναι ϵ-κοντά σε μία κατανομή με ελάχιστη εντροπία τουλάχιστον k_i.*

Το επόμενο λήμμα λέει ότι αν τα αρχικά τυχαία bits είναι $d = O(\log n)$ μπορούμε να τα πολλαπλασιάζουμε κατά μία σταθερά (c_{tiny}, χρησιμοποιώντας πηγή με ελάχιστη εντροπία $2d$.

Αυτό μπορεί να γίνει εάν χαλαρώσουμε την απαίτηση για pairwise independence,και επιτρέψουμε στην οικογένεια να έχει ένα μικρό σφάλμα σύγγρουσης, οπότε το μέγεθος της οικογένειας μπορεί να μειωθεί. Λεπτομέρειες μπορεί να βρει κανείς στα [16],[4].

Λήμμα 3 *[16] Υπάρχει σταθερά $c > 1$ τέτοια ώστε για κάθε $d = O(\log n)$ υπάρχει explicit $(2d, 2^{-d/5})$-extractor $A_d : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^{cd}$. Θα συμβολίζουμε αυτό το c ως c_{tiny}.*

Λήμμα 4 *[1][10] Έστω $X = (X_1, X_2, ..., X_t)$ μια $(k_1, ..., k_t)$ block-wise source με σφάλμα ϵ, όπου $k_t = \Omega(\log n)$ και $k_{i-1} = c_{tiny} k_i$. Τότε υπάρχει explicit block extractor $BExt(X, U_{k_t})$ που χρησιμοποιεί k_t τυχαία bits,και εξάγει $\Omega(\sum_{i=1}^{t} k_i)$ (σχεδόν) τυχαία bits,με σφάλμα $O(2^{-\Omega(k_t)} + t\varepsilon)$.*

Δηλαδή συνθέτοντας πολλούς extractors,τα αρχικά τυχαία bits πολλαπλασιάζονται κατά έναν παράγοντα ίσο με το γινόμενο των παραγόντων του κάθε extractor χωριστά.

3.3.2 Δημιουργία block wise source

Αυτό που χρειαζόμαστε τώρα είναι να κατασκευάσουμε μία block-wise source ,από μία πηγή με αρκετή ελάχιστη εντροπία, αφού είπαμε ότι μόνο αυτήν έχουμε στη διάθεσή μας.

Κατ' αρχάς πρέπει να φτιάξουμε ένα πρώτο block με αρκετή ελάχιστη εντροπία, που όμως να αφήνει και αρκετή για τα υπόλοιπα μπλοκ. Αποδεικνύεται ότι για αυτό αρκεί να διαλέξουμε μερικά από τα bits του X ανεξάρτητα ανά δύο. Το επόμενο λήμμα λέει ότι αν διαλέξουμε τυχαία l από τα n bits της πηγής, τότε με μεγάλη πιθανότητα, η ελάχιστη εντροπία που θα έχουν αυτά που θα πάρουμε θα είναι περίπου ένα ποσοστό l/n της εντροπίας της πηγής.

Οι αποδείξεις των λημμάτων βρίσκονται στα [10],[16].

Έστω ότι δίνεται μια συμβολοσειρά από n bits $x_1, ..., x_n$ και ένα υποσύνολο $S \subseteq \{1, ..., n\}$. Θα συμβολίζουμε ως x_S τη συμβολοσειρά $x_{i_1}x_{i_2}...$ για όλα τα $i \in S$, με τη σειρά όμως που είχαν στην αρχική συμβολοσειρά.

Λήμμα 5 *Για κάθε κατανομή X και για σχεδόν κάθε επιλογή του S, η κατανομή X_S είναι στατιστικά κοντά σε μία κατανομή W με $H_\infty(W) \geq \Omega(\frac{l}{n}H_\infty(X))$.*

Λήμμα 6 *Έστω X μία τυχαία πηγή πάνω στο $\{0,1\}^n$. Για κάθε $l > 0$ και $\delta > 0$ υπάρχει (explicitly, δηλαδή μπορούμε να την κατασκευάσουμε) μία συνάρτηση $B(x, y)$ που παίρνει ένα $x \in X$ και ένα μικρό ($O(\log n)$) τυχαίο y και επιστρέφει l bits έτσι ώστε αν $H_\infty(X) \geq \delta n$ τότε η $B(X, U)$ είναι $(\delta l)^{\Omega(-1)}$-κοντά σε μία κατανομή W με $H_\infty(W) \geq \Omega(\frac{\delta l}{\log(d^{-1})}) \geq \Omega(\frac{\delta l}{\log n})$.*

Δηλαδή μπορούμε να κατασκευάσουμε ένα πρώτο μπλοκ $B_1 = B(X, U)$ με αρκετή ελάχιστη εντροπία και μήκος έστω l_1. Επίσης αν $l_1 << k$, μένει αρκετή ελάχιστη εντροπία για τα υπόλοιπα, διότι για κάθε τιμή b_1 του B_1 ισχύει $H_\infty(X|B_1 = b_1) \geq H_\infty(X) + \log \Pr[B_1 = b_1]$ και $\Pr[B_1 = b_1]$ είναι κατά μέσον όρο 2^{l_1}. Αυτό σημαίνει ότι ακόμα και δεδομένων των bit του B_1, η X έχει αρκετή ελάχιστη εντροπία, οπότε μπορούμε να διαλέξουμε ένα δεύτερο μπλοκ B_2 με αρκετή ελάχιστη εντροπία, ακόμα και δεδομένου του B_1, κ.ο.κ. για τα υπόλοιπα μπλοκ B_i. Αρκεί $l_1 + l_2 + ... + l_{i-1} << k$.

Άρα έχουμε το εξής λήμμα.

Λήμμα 7 *Έστω X μιά κατανομή πάνω στο $\{0,1\}^n$ με $H_\infty(X) \geq k$. Τότε για κάθε επιλογή των $l_1, ...l_t$ όπου $\sum l_i < k/2$, η παραπάνω διαδικασία εξάγει μία πηγή $B = (B_1, ..., B_t)$ που είναι κοντά σε μία $(k_1, ..., k_t)$ block-wise source με $k_i = \Omega(kl_i/n)$.*

Παρατηρήστε ότι αυτό το λήμμα απαιτεί $k \geq \Omega(\sqrt{n})$ γιατί αλλιώς, αν $k \leq \sqrt{n}$ τότε για να έχω $k_1 \geq 1$ πρέπει $kl_1/n \geq 1 \Rightarrow l_1/\sqrt{n} \geq 1 \Rightarrow l_1 \geq \sqrt{n} \geq k$. Οπότε δεν μένει άλλη τυχαιότητα στην X για τα υπόλοιπα μπλοκ!

Στο [8] υπάρχει μία εναλλακτική μέθοδος, που εφαρμόζεται για κάθε k. Η βασική ιδέα, χρησιμοποιώντας την εντροπία Shannon αντί για την ελάχιστη εντροπία, είναι η εξής. Έστω $X = X_1...X_n$ και $H(X) \geq k$. Θέτω $e_i = H(X_1...X_i)$. Ισχύει $0 \leq e_i - e_{i-1} \leq 1$, $e_0 = 0$ και $e_n \geq k$. Άρα για k_1 (δεδομένο) υπάρχει $0 \leq i_1 \leq n$ τ.ω. $e_{i_1} = H(X_1...X_{i_1}) = k_1$. Το $X_1...X_{i_1}$ θα είναι το πρώτο μπλοκ. Τώρα $H(X_{i_1+1}...X_n|X_1...X_{i_1}) = H(X) - H(X_1...X_{i_1}) \geq k - k_1$. Άρα για k_2 υπάρχει $i_1 \leq i_2 \leq n$ τ.ω. $H(X_{i_1+1}...X_{i_2}) = k_2$ κ.ο.κ. μέχρι $\sum_j k_j = k$.

Η βασική ιδέα, δηλαδή, είναι ότι αν έχουμε μία συμβολοσειρά από n bits , με εντροπία k, μπορούμε να βρούμε ένα prefix αυτής με εντροπία k_1. Αυτό είναι το πρώτο μπλοκ. Η συμβολοσειρά που απομένει αν αφαιρέσουμε το πρώτο μπλοκ, έχει εντροπία $k - k_1$, δεδομένου του πρώτου μπλοκ, αρκετή ώστε να μπορούμε να βρούμε πάλι ένα prefix με εντροπία k_2, κ.ο.κ.

Αυτή η ιδέα σε γενικές γραμμές εφαρμόζεται στο [8] θεωρώντας την ελάχιστη εντροπία. Οπότε παίρνουμε μία block-wise πηγή.

Η εύρεση των $i_1, i_2, ...$ κατασκευαστικά, εξαρτάται από την κατανομή X.

3.3.3 Μερικές κατασκευές

Κατασκευάζουμε μία σχεδόν block-wise source από $t = O(\log n)$ blocks , μεγέθους $l_i = O(k/\log n)$. Ξεκινάμε με $O(\log n)$ τυχαία bits . Κάθε μπλοκ έχει ελάχιστη εντροπία $k_i = \Omega(kl_i/n) = \Omega(k^2/n \log n)$. Οπότε από το λήμμα 4 υπάρχει block extractor που βγάζει $\Omega(\sum_{i=1}^{t} k_i) = \Omega(\log n \cdot k^2/n \log n) = \Omega(k^2/n)$ (σχεδόν) τυχαία bits .

Τα τυχαία bits που χρειαζόμαστε, είναι $O(\log n)$ για το seed του block-extractor , και $O(\log n)$ για τη δημιουργία του κάθε μπλοκ (από το λήμμα 6). Αλλά έχουμε $t = O(\log n)$ blocks . Άρα χρειαζόμαστε συνολικά $d = O(\log^2 n)$ τυχαία bits .

Επίσης, όπως είπαμε προηγουμένως, αυτό γίνεται για $k = \Omega(\sqrt{n})$.

Άρα έχουμε το εξής λήμμα.

Λήμμα 8 *Έστω $k(n) \geq n^{\frac{1}{2}+\gamma}$ για κάποια σταθερά $\gamma > 0$. Για κάθε ϵ μπορούμε να κατασκευάσουμε έναν (k, ϵ)-extractor $E : \{0,1\}^n \times \{0,1\}^{O(\log^2 n \cdot \log \frac{1}{\epsilon})} \rightarrow \{0,1\}^{\frac{k^2}{n}}$.*

Μπορούμε να εξάγουμε $m = \Omega(n)$ bits , αν $k = \Omega(n)$.

Μείωση του d

Μπορούμε να μειώσουμε το d από $O(\log^2 n)$ σε $O(\log n)$ ως εξής.

Κατασκευάζουμε δύο μπλοκ, το ένα μήκους $k/2$ και το άλλο μήκους $n' = 2^{O(\sqrt{\log n})}$.

Για το δεύτερο κατασκευάζουμε έναν block-extractor, όπως περιγράψαμε πρίν, που χρησιμοποιεί $O(\log^2 n') = O(\log n)$ τυχαία bits , και εξάγει $m' > O(\log^2 n)$ bits .

Τώρα κατασκευάζουμε έναν block extractor για το πρώτο μπλοκ, και χρησιμοποιούμε για τυχαία bits τα m' που εξάγαμε.

Οπότε συνολικά χρησιμοποιούμε $2O(\log n)$ τυχαία bits για την κατασκευή των πρώτων δύο μπλοκ, και $O(\log n)$ για την είσοδο του πρώτου extractor .

Αποδεικνύεται [16, 8] ότι αρκούν $d = O(\log n + \log \epsilon^{-1})$ τυχαία bits για κάθε ϵ και $k = \Omega(n)$.

Αύξηση του m

Αφού εξάγουμε m_1 bits χρησιμοποιώντας d_1 τυχαία bits και μια πηγή X με ελάχιστη εντροπία k, τότε αν κάποιος extractor μπορεί να εξάγει από μία πηγή με ελάχιστη εντροπία $k - m_1$, μπορούμε να τον χρησιμοποιήσουμε πάλι για να εξάγουμε m_2 bits από τη X, χρησιμοποιώντας άλλα d_2 τυχαία bits (προσοχή να είναι ανεξάρτητα από τα προηγούμενα). Αυτό γιατί η X (σχεδόν πάντα) ακόμα και δεδομένων των m_1 bits , έχει ακόμα ελάχιστη εντροπία $k - m_1$.

Το ίδιο μπορούμε να επαναλάβουμε πολλές φορές, οπότε χρησιμοποιώντας $\sum d_i$ τυχαία bits , εξάγουμε $\sum m_i$ bits , όσο το $k - \sum m_{i-1}$ είναι αρκετό.

Για κάθε $\eta > 0$ και $k = \Omega(n)$ μπορούμε να εξάγουμε $m = k(1 - \eta)$ bits , επαναλαμβάνοντας την παραπάνω κατασκευή $O(1)$ φορές, και χρησιμοποιώντας $d = O(\log n)$ πραγματικά τυχαία bits [8].

Κεφάλαιο 4

Trevisan's Extractor

Nisan-Wigderson generator

Η Nisan-Wigderson (NW) γεννήτρια ψευδοτυχαίων αριθμών χρησιμοποιεί μια boolean συνάρτηση $f : \{0,1\}^l \to \{0,1\}$ που είναι δύσκολο να προσεγγιστεί,(δεν γίνεται να προσεγγιστεί από κύκλωμα μικρού μεγέθους, και θα δώσουμε αργότερα ακριβείς ορισμούς), και υπολογίζει την τιμή της σε πολλά τυχαία σημεία. Τα bits που παράγει φαίνονται τυχαία σε έναν υπολογιστικά περιορισμένο αντίπαλο.

Για να διαλέξει τα τυχαία σημεία στα οποία θα υπολογίσει την τιμή της f χρειάζεται μερικά πραγματικά τυχαία bits . Εάν θέλαμε τα σημεία να τα επιλέξουμε ανεξάρτητα, θα χρειαζόμασταν l bits για την επιλογή του κάθε σημείου.

Για να μειώσουμε τα τυχαία bits που θα χρειαστούν συνολικά, διαλέγουμε τα σημεία όχι τελείως ανεξάρτητα, αλλά με μία μικρή εξάρτηση, χρησιμοποιώντας ένα σχεδιασμό. Τελικά αποδεικνύεται ότι παρά αυτήν την εξάρτηση, το αποτέλεσμα της γεννήτριας εξακολουθεί να φαίνεται τυχαίο σε έναν χρονικά περιορισμένο αντίπαλο.

Η απόδειξη δείχνει ότι για κάθε f για την οποία το αποτέλεσμα της γεννήτριας μπορεί να διακριθεί από το τυχαίο string , (δηλαδή η κατανομή που ακολουθεί το αποτέλεσμα μπορεί να διακριθεί από την ομοιόμορφη), μπορούμε να βρούμε μία συνάρτηση g που την προσεγγίζει, (δηλαδή υπάρχει κύκλωμα μικρού μεγέθους που υπολογίζει τη g). Αυτό όμως είναι αντίφαση, αφού η f θεωρήσαμε ότι είναι δύσκολο να προσεγγιστεί.

Επιπλέον αποδεικνύεται ότι η g ανήκει σε μία οικογένεια G, που είναι ανεξάρτητη από την f, και είναι μικρή. (Εξαρτάται όμως από τον αντίπαλο. Δηλαδή για κάθε αντίπαλο T έχουμε μια μικρή οικογένεια G_T, που τα g που

περιέχει προσεγγίζουν κάθε f για το οποίο η NW_f γεννήτρια δίνει αποτέλεσμα που ο T μπορεί να το διακρίνει από το τυχαίο).

Trevisan's Extractor

Ο Trevisan παίρνει την NW γεννήτρια , και λέει: αντί να χρησιμοποιήσουμε μια δύσκολο να προσεγγιστεί συνάρτηση f, να χρησιμοποιήσουμε μία τυχαία συνάρτηση x από μία πηγή X με κάποια ελάχιστη εντροπία. Δηλαδή θεωρούμε κάθε $x \in X$ σαν τον πίνακα αληθοτιμών μιας συνάρτησης f (δηλαδή σαν την παράθεση $f(1)...f(n)$ των τιμών της, όπου $n = 2^l$).

Και τώρα κοιτάμε πόσο τυχαίο είναι το αποτέλεσμα της γεννήτριας, για το τυχαίο x από την X. Εάν η κατανομή που ακολουθεί (το αποτέλεσμα) είναι κοντά στην ομοιόμορφη, τότε έχουμε extractor .

Οπότε για να έχουμε extractor πρέπει το αποτέλεσμα της γεννήτριας για το τυχαίο x από την X, και το πραγματικά τυχαίο y να μην διακρίνεται από μία τυχαία συμβολοσειρά.

Για κάθε αντίπαλο T, χωρίζουμε τα $x \in X$ σε "καλά" και "κακά". Τα "κακά" είναι αυτά για τα οποία ο T διακρίνει το αποτέλεσμα από το τυχαίο, και τα "καλά" είναι αυτά για τα οποία δεν το διακρίνει.

Για να έχουμε extractor πρέπει τα "κακά" να είναι λίγα.

Για να μετρήσουμε λοιπόν τα "κακά" x σκεφτόμαστε το εξής. Για κάθε κακό x , (από την ανάλυση της NW γεννήτριας), έχουμε ένα g από την μικρή οικογένεια G_T, που το προσεγγίζει. Εννοούμε ότι το g και το x συμφωνούν σε περισσότερα από τα μισά σημεία (bits) , ή αλλιώς έχουν σχετική απόσταση Hamming μικρότερη από 1/2.

Κάθε "κακό" x προσεγγίζεται από ακριβώς ένα g. Εάν συνέβαινε και το αντίστροφο, δηλαδή εάν και κάθε g προσέγγιζε το πολύ ένα x, τότε το πλήθος των κακών x θα ήταν το πολύ όσο το πλήθος των g, δηλ. $\mid G_T \mid$.

Όμως κάθε g μπορεί να προσεγγίσει περίσσότερα από ένα x, ας πούμε λ το πλήθος. Οπότε τα κακά x είναι το πολύ $\lambda \cdot \mid G_T \mid$.

Δυστυχώς το λ είναι πολύ μεγάλο, πάνω από $\binom{n}{n/2}$, (το πλήθος των συμβολοσειρών που έχουν σχετική απόσταση Hammimg το πολυ 1/2 από το g).

Η λύση είναι να χρησιμοποιήσουμε έναν κώδικα διόρθωσης λαθών. Οι κώδικες διόρθωσης λαθών "απομακρύνουν" τις λέξεις μεταξύ τους, έτσι ώστε κάθε σφαίρα ακτίνας μικρότερης του 1/2, (οπότε και η σφαίρα γύρω από το g), έχει πολύ λίγα στοιχεία. Άρα το λ τώρα είναι μικρό.

Οπότε, έστω C ένας κώδικας διόρθωσης λαθών με την παραπάνω ιδιότητα, και θεωρώντας το $C(x)$ σαν τον αληθοπίνακα μιας boolean συνάρτησης, να τι έχουμε τελικά: Αν η NW_f γεννήτρια ορίζεται ως

$$NW_f(y) = f(y_1)...f(y_m) = f_{|y_1}...f_{|y_m}$$

με τα y_i τυχαία, ο extractor του Trevisan ορίζεται ως

$$Ext(x,y) = NW_{C(x)}(y) = C(x)_{|y_1}...C(x)_{|y_m}$$

$$x \in X$$

Δηλαδή στη θέση της δύσκολα προσεγγίσιμης f, χρησιμοποιούμε, όχι αυτούσια ένα τυχαίο x από μία πηγή X με κάποια ελάχιστη εντροπία k, αλλά το $C(x)$, όπου C ένας κώδικας διόρθωσης λαθών με την επιθυμητή ιδιότητα.

Στο τέλος διαλέγουμε κατάλληλα τις παραμέτρους ώστε να έχουμε $(k, 2\varepsilon)$-extractor.

4.1 Κώδικες Διόρθωσης Λαθών

4.1.1 Βασικοί ορισμοί

Ορισμός 17 *Ένας q-αδικός κώδικας είναι ένα σύνολο $C \subseteq \Sigma^{\hat{n}}$, όπου το Σ είναι ένα αλφάβητο μεγέθους q. Τα στοιχεία του C λέγονται κωδικές λέξεις. Μια συνάρτηση κωδικοποίησης είναι μία συνάρτηση $Enc : \{0,1\}^n \to C$ όπου $n = log|C|.(n < \hat{n})$*

Ορισμός 18 *Για δύο συμβολοσειρές $x, y \in \Sigma^{\hat{n}}$, η σχετική τους απόσταση Hamming $d_H(x,y)$είναι ίση με $\Pr_i[x_i \neq y_i]$. Για μια συμβολοσειρά $x \in \Sigma^{\hat{n}}$ και $\delta \in [0,1]$, η μπάλα Hamming ακτίνας δ γύρω από το x είναι το σύνολο $B(x,\delta)$ των συμβολοσειρών $y \in \Sigma^{\hat{n}}$ για τις οποίες $d_H(x,y) \leq \delta$.*

Ορισμός 19 *Η ελάχιστη σχετική απόσταση ενός κώδικα $C \subseteq \Sigma^{\hat{n}}$ είναι ίση με $min_{x \neq y \in C} d_H(x,y)$.*

Ορισμός 20 *Έστω $Enc : \{0,1\}^n \to C$ ένας αλγόριθμος κωδικοποίησης για έναν κώδικα C. Ένας (δ, L)-list-decoding αλγόριθμος για την Enc είναι μία συνάρτηση $Dec : \Sigma^{\hat{n}} \to (\{0,1\}^n)^L$ τ.ω. για κάθε $m \in \{0,1\}^n, r \in \Sigma^{\hat{n}}$ τ.ω. $d\_H(Enc(m), r) \leq \delta$, έχουμε ότι $m \in Dec(r)$. Αν ένας τέτοιος σλγόριθμος υπάρχει, λέμε ότι ο κώδικας είναι (δ, L)-list-decodable.*

Πρόταση 8 *Έστω ένας κώδικας $C \subseteq \Sigma^{\hat{n}}$ με οποιαδήποτε συνάρτηση κωδικοποίησης. Ο C είναι (δ, L)-list-decodable αν για κάθε $r \in \Sigma^{\hat{n}}$ έχουμε $|B(r,\delta) \cap C| \leq L$.*

Η επόμενη πρόταση είναι πολύ σημαντική. Λέει ότι αν ένας κώδικας διόρθωσης λαθών έχει ελάχιστη απόσταση $1-\epsilon$, τότε κάθε μπάλα ακτίνας $1/2-\sqrt{\epsilon}$ έχει το πολύ $1/\epsilon$ κωδικές λέξεις.

Πρόταση 9 *(Johnson Bound))*

1. *Αν ο C έχει ελάχιστη απόσταση $1-\epsilon$, τότε είναι $(1-O(\sqrt{\epsilon}), O(1/\sqrt{\epsilon}))$-list-decodable.*

2. *Αν ένας διαδικός κώδικας C έχει ελάχιστη απόσταση $1/2-\epsilon/2$, τότε είναι $(1/2-\sqrt{\epsilon}, 1/\epsilon)$-list-decodable.*

ΑΠΟΔΕΙΞΗ. Θα αποδείξουμε το 1, και το 2 γίνεται ομοίως. Η απόδειξη είναι με την αρχή του εγκλεισμού-αποκλεισμού. Έστω $r \in \Sigma^{\hat{n}}$, και έστω ότι $C_1, ..., C_s$ είναι κωδικές λέξεις με απόσταση το πολύ $1-\epsilon'$ από το r, για $\epsilon' = \sqrt{2\epsilon}$ και $s = 2/\epsilon'$.

$$\begin{aligned} 1 &\geq \text{ποσοστό των θέσεων όπου το r συμφωνεί με κάποιο } C_i \\ &\geq \sum_i agreement(r, C_i) - \sum_{1 \leq i \leq j \leq s} agreement(C_i, C_j) \\ &\geq s\epsilon' - \binom{s}{2} \cdot \epsilon \\ &> 2 - 1 = 1 \end{aligned}$$

όπου η τελευταία ανισότητα προκύπτει από την επιλογή των παραμέτρων που κάναμε. Προκύπτει άτοπο, άρα $s < 2/\epsilon'$. ■

4.1.2 Κατασκευές

Hadamard Codes

- Αλφάβητο: $\Sigma = \{0, 1\}$.
- Κωδικοποίηση: $Had_y(x) = \sum_i x_i y_i \mod 2$ δηλ. το y-οστό ψηφίο του $Had(x)$ είναι το εσωτερικό γινόμενο των $x, y \mod 2$.
- Μήκος κωδικών λέξεων: $\hat{n} = 2^n$.
- Ελάχιστη (σχετική) απόσταση: $\delta = 1/2$.

Reed-Solomon Codes

- Αλφάβητο: $\Sigma = GF(2^m)$, δηλ. το πεπερασμένο πεδίο μεγέθους 2^m ($|\Sigma| = 2^m$), με στοιχεία όλα τα πολώνυμα βαθμού $m-1$ με συντελεστές από το $\mathbb{Z}_2$. Για την περιγραφή του αρκεί να βρεθεί ένα ανάγωγο πολυώνυμο βαθμού m. Γενικότερα $\Sigma = F_q$ πεπερασμένο πεδίο μεγέθους $q = p^m$ με p πρώτο.

- Κωδικοποίηση: Θεωρούμε το $x \in \{0,1\}^n$ να δίνει τους συντελεστές ενός πολυωνύμου $p_x : F_q \to F_q$ βαθμού το πολύ d, όπου $n = (d+1) \cdot \log q$. Η κωδικοποίηση είναι η εξής

$$C(x) = (p_x(a_1), ..., p_x(a_{|\Sigma|}))$$

  όπου $a_1, ..., a_{|\Sigma|} \in F_q = \Sigma$.

- Μήκος κωδικών λέξεων: $\hat{n} = q$.

- Ελάχιστη (σχετική) απόσταση: $\delta = 1 - d/q$.

Code Concatenation

Για τον extractor του Trevisan χρειαζόμαστε έναν κώδικα διόρθωσης λαθών με μεγάλη σχετική απόσταση Hamming. Κατ' αρχάς οι κώδικες Hadamard έχουν σχετική απόσταση $1/2$ μεταξύ οποιονδήποτε δυό κωδικών λέξεων, αλλά οι λέξεις έχουν πολύ μεγάλο μήκος $\hat{n} = 2^n$, ενώ θα προτιμούσαμε μήκος $\hat{n} = poly(n)$.

Οι καλύτεροι κώδικες που έχουν βρεθεί είναι οι Reed-Solomon, με ελάχιστη απόσταση $\delta = 1 - 1/n^{\Omega(1)}$ και μήκος $\hat{n} = poly(n)$.

Το πρόβλημα που προκύπτει, όμως, είναι ότι το αλφάβητο Σ των Reed-Solomon κωδίκων δεν είναι δυαδικό, και η ελάχιστη απόσταση αναφέρεται στις λέξεις αυτού του αλφάβητου. Οπότε αν π.χ. δύο κωδικές λέξεις μήκους $\hat{n}$ διαφέρουν σε τουλάχιστον $\hat{n} - d$ σύμβολα του Σ, θα σήμαινε ότι μπορούν να διορθωθούν μέχρι $\frac{\hat{n}-d}{2}$ λάθη.

Όταν, όμως, η λέξη εκφραστεί σε δυαδικό σύστημα, τότε κάθε σύμβολο του Σ έχει μήκος $\log|\Sigma|$, και θα έπρεπε να μπορούν να διορθωθούν μέχρι $\frac{\hat{n}-d}{2} \cdot \log|\Sigma|$ λάθος bits. Αυτό, όμως δεν συμβαίνει, γιατί τα λάθος bits μπορεί να είναι σκορπισμένα παντού, και να αλλάζουν περισσότερα από $\frac{\hat{n}-d}{2}$ σύμβολα του Σ.

Θα έπρεπε, με άλλα λόγια, όταν κάποιος αντίπαλος αλλάζει $\log|\Sigma|$ bits της κωδικής λέξης, να αλλάζει μόνο αυτά που αντιστοιχούν σε ένα μόνο σύμβολο του Σ. Όμως τίποτα δεν τον αναγκάζει να το κάνει αυτό, και μπορεί να τα σκορπίσει και να αλλάξει έτσι κι άλλα σύμβολα του Σ.

Η λύση είναι η εξής. Σε κάθε σύμβολο του Σ, αφού το μετατρέψουμε σε δυαδικό σύστημα, να του εφαρμόσουμε έναν κώδικα Hadamard, ο οποίος έχει σχετική απόσταση 1/2, που σημαίνει ότι για να αλλάξει ο αντίπαλος ένα σύμβολο του Σ, θα πρέπει να αλλάξει τουλάχιστον τα μισά από τα bit που αντιστοιχούν σε αυτό το σύμβολο.

Αυτή η διαδικασία, που λέγεται Code Concatenation ενός Reed-Solom με έναν Hadamard κώδικα, είναι πολύ έξυπνη και χρήσιμη, και μας δίνει το επόμενο θεώρημα.

Θεώρημα 21 *Για κάθε $n \in \mathbb{N}, \delta > 0$, υπάρχει ένας κώδικας $EC : \{0,1\}^n \to \{0,1\}^{\hat{n}}$ με $\hat{n} = poly(n, \frac{1}{\delta})$ και ελάχιστη σχετική απόσταση $\frac{1}{2} - \frac{\delta^2}{2}$.*

ΑΠΟΔΕΙΞΗ. Εάν δίνονται οι παράμετροι n και δ, έστω $m = \lceil \log(n/\delta^2) \rceil$.

Έστω $Had : \{0,1\}^m \to \{0,1\}^{2^m}$ ο κώδικας Hadamard .

Έστω $F = GF(2^m)$ ($|F| = 2^m$). Μια περιγραφή του F μπορεί να βρεθεί σε χρόνο $poly(2^m) = poly(n, 1/\delta)$, αναζητώντας εξαντλητικά ένα ανάγωγο πολυώνυμο βαθμού m πάνω στο $GF(2)$.

Μπορούμε να θεωρήσουμε ότι τα $x \in \{0,1\}^n \subset (\{0,1\}^m)^{\lceil n/m \rceil}$ δίνουν τους συντελεστές ενός πολυωνύμου p_x πάνω στο F, βαθμού το πολύ $d = \lceil n/m \rceil$.

Ορίζουμε τον κώδικα διόρθωδης λαθών $EC : \{0,1\}^n \to (\{0,1\}^{2^m})^{|F|}$ ως

$$EC(x) = (Had(p_x(a_1)), ..., Had(p_x(a_{|F|}))),$$

όπου $a_1, ..., a_{|F|}$ είναι όλα τα στοιχεία του F. Οπότε οι κωδικές λέξεις έχουν μήκος $\bar{n} = 2^m \cdot |F| = 2^{2m} = O(n^2/\delta^4)$.

Τώρα θα υπολογίσουμε την ελάχιστη απόσταση αυτού του κώδικα. Για δύο διαφορετικά στοιχεία $x, y \in \{0,1\}^n$, τα p_x και p_y διαφέρουν σε τουλάχιστον $|F| - d$ στοιχεία του F (επειδή είναι διαφορετικά πολυώνυμα βαθμού d).

Για κάθε a τ.ω. $p_x(a) \neq p_y(a)$, τα $Had(p_x(a))$ και $Had(p_y(a))$ διαφέρουν σε $2^m/2$ θέσεις (ιδιότητα του Hadamard).

Άρα για δύο διαφορετικά x και y, τα $EC(x)$ και $EC(y)$ διαφέρουν σε τουλάχιστον $q = (|F| - d) \cdot 2^m/2$ θέσεις, δίνοντας σχετική απόσταση

$$\frac{q}{|F| \cdot 2^m} = \frac{1}{2} - \frac{d}{2|F|} \geq \frac{1}{2} - \frac{\delta^2}{2}.$$

■

Συνδιάζοντας το προηγούμενο θεώρημα με την πρόταση 9 (Johnson Bound),ποψ λέει ότι αν ένας κώδικας διόρθωσης λαθών έχει ελάχιστη απόσταση $1-\epsilon$, τότε κάθε μπάλα ακτίνας $1/2 - \sqrt{\epsilon}$ έχει το πολύ $1/\epsilon$ κωδικές λέξεις, για $\epsilon = \delta^2$, παίρνουμε το εξής λήμμα, που θα χρειαστούμε στην απόδειξη του extractor του Trevisan.

Λήμμα 9 *(Κώδικες διόρθωσης λαθών) Για κάθε n και δ υπάρχει μία πολυωνυμικού χρόνου υπολογίσιμη κωδικοποίηση $EC : \{0,1\}^n \to \{0,1\}^{\overline{n}}$ όπου $\overline{n} = poly(n, \frac{1}{\delta})$ τ.ω. κάθε μπάλα με ακτίνα Hamming $(\frac{1}{2} - \delta)\overline{n}$ στο $\{0,1\}^{\overline{n}}$ περιέχει το πολύ $\frac{1}{\delta^2}$ κωδικές λέξεις. Επιπλέον το $\overline{n}$ μπορεί να θεωρηθεί δύναμη του 2.*

4.2 Σχεδιασμοί

4.2.1 Σχεδιασμοί

Ορισμός 22 *(Σχεδιασμός) Για θετικούς ακέραιους $m, l, \alpha \leq l, t \geq l$, ένας (m, t, l, a) σχεδιασμός είναι μία οικογένεια συνόλων $S = \{S_1, ..., S_m\}$ τ.ω.*
-$S_i \subseteq [t]$
-$|S_i| = l$
-Για κάθε $i \neq j \in [m], |S_i \cap S_j| \leq \alpha$.

Λήμμα 10 *(Κατασκευή σχεδιασμού) Για κάθε θετικούς ακέραιους $m, l, \alpha \leq l$ υπάρχει ένας (m, t, l, α) σχεδιασμός, όπου $t = e^{\frac{lnm}{a}} \frac{l^2}{\alpha}$ και μπορεί να υπολογιστεί ντετερμινιστικά σε χρόνο $O(2^t m)$.*

ΑΠΟΔΕΙΞΗ. Για την απόδειξη θα χρησιμοποιήσουμε το εξής Chernoff bound [6].

Λήμμα 11 *Έστω $X_1, ..., X_n$ ανεξάρτητες τυχαίες μεταβλητές $0, 1$, τέτοιες ώστε $E[\sum_i X_i] = \mu$. Τότε για κάθε $\alpha > 1$ ισχύει*

$$\Pr[\sum_i X_i \geq \alpha\mu] \leq e^{-((ln\alpha)+\frac{1}{\alpha}-1)\alpha\mu}.$$

Θεωρούμε ότι το $[t]$ αποτελείται από l διαστήματα $I_i, i = 1, ..., l$, κάθε ένα μεγέθους t/l.

Κατασκευάζουμε με τη σειρά m υποσύνολα $S_j \subset [t], j = 1, ..., m$, έτσι ώστε κάθε ένα να περιέχει ακριβώς ένα στοιχείο από κάθε διάστημα I_i, και επιπλέον να έχει τομή μεγέθους το πολύ α με κάθε προηγούμενο υποσύνολο που έχουμε διαλέξει.

Σε κάθε βήμα μπορούμε να βρούμε ένα υποσύνολο με τις παραπάνω επιθυμητές ιδιότητες, και αυτό αποδεικνύεται με ένα πιθανοτικό επιχείρημα.

Λήμμα 12 *Έστω $S_1, ..., S_k$, $k < m$ μία συλλογή από υποσύνολα του $[l]$ τ.ω. $| S_i \cap S_j | \leq \alpha$, $i \neq j$. Τότε υπάρχει ένα σύνολο $S \subset [t]$, που περιέχει ένα στοιχείο από κάθε διάστημα I_i, $i = 1, ..., l$ και $| S \cap S_j | \leq \alpha$ για κάθε $j = 1, ..., k$.*

ΑΠΟΔΕΙΞΗ. Διαλέγουμε το S τυχαία, δηλαδή διαλέγουμε στην τύχη ένα στοιχείο από κάθε διάστημα, και το βάζουμε στο S.

Ορίζουμε τις τυχαίες μεταβλητές $X_i,\ i = 1, ..., l$ ως εξής

$$X_i = \begin{cases} 1 & \text{αν τα } S \text{ και } S_i \text{ έχουν κοινό στοιχείο από το } I_i \\ 0 & \text{αλλιώς} \end{cases}$$

Οπότε έχουμε

$$\mid S \cap S_j \mid = X_1 + ... + X_i = \sum_i X_i$$

Επίσης κάθε I_i έχει t/l στοιχεία, και για το S διαλέγουμε ένα απόαυτά στην τύχη, οπότε

$$E[X_i] = \frac{1}{t/l} = \frac{l}{t},\ \forall i = 1, ..., l$$

Άρα

$$\mu = E[\mid S \cap S_j \mid] = E[\sum_i X_i] = \sum E[X_i] = \frac{l^2}{t}$$

Οπότε από το λήμμα 11 έχουμε

$$\begin{aligned} \Pr[\mid S \cap S_j \mid > \alpha] = \\ \Pr[\sum_i X_i > (\frac{\alpha}{\mu})\mu] \leq \\ e^{-((\ln \frac{\alpha}{\mu}) + \frac{\mu}{\alpha} - 1)} < \\ e^{-\alpha(\ln \frac{\alpha}{m} - 1)} = \frac{1}{m} \end{aligned}$$

η τελευταία ισότητα ισχύει επειδή $\frac{\alpha}{\mu} = \frac{\alpha t}{l^2}$ και $t = \frac{l^2}{\alpha} e^{\frac{\ln m}{\alpha}}$.
(Ή αλλιώς, επειδή θέλουμε να βγει $1/m$, προκύπτει ότι πρέπει $t = \frac{l^2}{\alpha} e^{\frac{\ln m}{\alpha}}$).

Άρα

$$\Pr[\exists i \in \{1, ..., k\} \text{ τ.ω. } \mid S \cap S_j \mid > \alpha] \leq \frac{k}{m} < 1$$

Δηλαδή η πιθανότητα το τυχαίο S να έχει μεγάλη τομή ($> \alpha$) με κάποιο S_j είναι μικρότερη της μονάδας, άρα υπάρχει ένα S που έχει μικρή τομή με όλα τα S_j. ■

Το σύνολο S μπορεί να βρεθεί σε χρόνο $poly(2^t, m)$, δοκιμάζοντας όλα τα δυνατά υποσύνολα που έχουν ένα στοιχείο από κάθε I_i. ■

Η επόμενη πρόταση δίνει ένα κάτω φράγμα για το μέγεθος του t (του σύμπαντος του σχεδιασμού).

Πρόταση 10 *[12] Αν $S_1, ...S_m \subset [t]$ είναι ένας (m, t, l, α)-σχεδιασμός, τότε $m \leq \binom{t}{\alpha}/\binom{l}{\alpha}$. Ειδικότερα*

$$t \geq m^{\frac{1}{\alpha+1}} \cdot (l - \alpha).$$

4.2.2 Ασθενείς Σχεδιασμοί

Ορισμός 23 *(Ασθενής Σχεδιασμός) Για θετικούς ακεραίους $m, l, \rho, t \geq l$, ένας (m, t, l, ρ) ασθενής (weak) σχεδιασμός είναι μία οικογένεια συνόλων $S = \{S_1, ..., S_m\}$ τ.ω. $\forall i \in [m]$*
-$S_i \subseteq [t]$
-$|S_i| = l$
-$\sum_{j<i} 2^{|S_i \cap S_j|} \leq \rho(m-1)$.

Προφανώς ένας (m, t, l, α) σχεδιασμός είναι και $(m, t, l, \underbrace{2^\alpha}_{\rho})$ ασθενής σχεδιασμός, αλλά όχι το αντίθετο. Αποδεικνύεται ότι είναι δυνατόν το t για έναν ασθενή σχεδιασμό να είναι πολύ μικρότερο απ΄ ότι του απλού σχεδιασμού. Αυτό, όπως θα δούμε παρακάτω, επιρρεάζει το μέγεθος του seed του extractor του Trevisan .

Ακολουθεί η κατασκευή ασθενούς σχεδιασμού.

Λήμμα 13 *(Κατασκευή ασθενούς σχεδιασμού) Για κάθε θετικούς ακέραιους $m, l \in \mathbb{N}, \rho > 1$ υπάρχει ένας (m, t, l, ρ) ασθενής σχεδιασμός, όπου $t = \lceil \frac{l}{\ln \rho} \rceil \cdot l$ και μπορεί να υπολογιστεί ντετερμινιστικά σε χρόνο $poly(m, t)$.*

ΑΠΟΔΕΙΞΗ. Έστω l, m, ρ δεδομένες παράμετροι, και έστω $t = \lceil \frac{l}{\ln \rho} \rceil \cdot l$. Θεωρούμε το $[t]$ σαν την ένωση l ξένων μεταξύ τους διαστημάτων $B_1, ..., B_l$, το καθένα μεγέθους $\lceil \frac{l}{\ln \rho} \rceil$. Κατασκευάζουμε τα σύνολα $S_1, ..., S_m$ στη σειρά έτσι ώστε

1. Κάθε σύνολο περιέχει ακριβώς ένα στοιχείο από κάθε διάστημα και
2. $\sum_{j<i} 2^{|S_i \cap S_j|} \leq \rho(i-1)$.

ΥΠΑΡΞΗ. Υποθέτουμε ότι έχουμε επιλέξει τα $S_1, ...S_{i-1} \subset [t]$ έτσι ώστε να ικανοποιούν τις δυό παραπάνω συνθήκες. Θα αποδείξουμε ότι υπάρχει ένα σύνολο S_i που ικανοποιεί τις παραπάνω συνθήκες, χρησιμοποιώντας την πιθανοτική μέθοδο. Έστω ότι διαλέγουμε το S_i τυχαία, δηλαδή διαλέγουμε ομοιόμορφα τυχαία κάποια στοιχεία $a_1, ..., a_l$ από τα διαστήματα $B_1, ..., B_l$ αντίστοιχα, και θέτουμε $S_i = \{a_1, ..., a_l\}$. Θα δείξουμε ότι η συνθήκη 2 ισχύει με μη μηδενική πιθανότητα, για τό τυχαίο S_i.

Ορίζουμε τις τυχαίεες μεταβλητές $U_{j,k},\ i = 1, ..., l$ ως εξής

$$Y_{j,k} = \begin{cases} 1 & \text{αν } a_k \in Sj \\ 0 & \text{αλλιώς} \end{cases}$$

έτσι για j σταθερό έχουμε

$$E_k[y_{j,k}] = \Pr[Y_{j,k} = 1] = \frac{1}{|B_k|} = \frac{1}{\lceil \frac{l}{\ln \rho} \rceil}$$

Για σταθερό j τα $Y_{j,1}, ..., Y_{j,l}$ είναι ανεξάρτητα.

$$\begin{aligned} & E_{S_i}[\sum_{j<i} 2^{|S_i \cap S_j|}] \\ &= \sum_{j<i} E_k[2^{\sum_k Y_{j,k}}] \\ &= \sum_{j<i} E_k[\prod_k 2^{Y_{j,k}}] \\ &= \sum_{j<i} \prod_{k=1}^{l} E_k[2^{Y_{j,k}}] \\ &= \sum_{j<i} \prod_{k=1}^{l} E_k[1 + Y_{j,k}] \\ &= (i-1)\big(1 + \frac{1}{\lceil l/\ln \rho \rceil}\big)^l \\ &\leq (i-1)\rho \end{aligned}$$

(Ή αλλιώς, για να έχω $(1 + \frac{1}{\lceil l/\ln \rho \rceil})^l \leq \rho$ αρκεί $|B_k| = \lceil l/\ln \rho \rceil$.)

Αφού η μέση τιμή που υπολογίσαμε είναι πάνω σε όλες τις πιθανές επιλογές του S_i, άρα υπάρχει μία επιλογή του S_i για την οποία η συνθήκη 2 ισχύει.

Τώρα θα κατασκευάσουμε ντετερμινιστικά ένα τέτοιο σύνολο, με τη μέθοδο των δεσμευμένων μέσων τιμών.

ΚΑΤΑΣΚΕΥΗ. Δείξαμε ότι $E_{S_i}[\sum_{j<i} 2^{|S_i \cap S_j|}] \leq (i-1)\rho$. Δεσμεύοντας ως προς a_1 προκύπτει ότι υπάρχει ένα $\alpha_1 \in B_1$ τέτοιο ώστε

$$E[\sum_{j<i} 2^{|S_i \cap S_j|} | a_1 = \alpha_1] \leq (i-1)\rho$$

Οπότε, αν μπορούμε γρήγορα να υπολογίσουμε τη δεσμευμένη μέση τιμή

$$E[\sum_{j<i} 2^{|S_i \cap S_j|} | a_1 = \alpha_1]$$

για κάθε $\alpha_1 \in B_1$, μπορούμε να βρούμε το α_1 για το οποίο ισχύει η προηγούμενη ανισότητα.

Με τον ίδιο τρόπο μπορούμε να βρούμε ένα $\alpha_2 \in B_2$ για το οποίο

$$E[\sum_{j<i} 2^{|S_i \cap S_j|} | a_1 = \alpha_1, a_2 = \alpha_2] \leq (i-1)\rho$$

και ομοίως να βρούμε και τα υπόλοιπα στοιχεία του συνόλου που ψάχνουμε.

Για να υλοποιήσουμε αυτόν τον αλγόριθμο πρέπει, όπως είπαμε ήδη, να μπορούμε να υπολογίσουμε εύκολα τις δεσμευμένες μέσες τιμές. Αποδεικνύεται με τρόπο ίδιο με τον υπολόγισμό της αδέσμευτης μέσης τιμής που κάναμε προηγουμένως, ότι για κάθε r θέτοντας $T = \{\alpha_1, ..., \alpha_r\}$

$$E\big[\sum_{j<i} 2^{|S_i \cap S_j|} | a_1 = \alpha_1, ..., a_r = \alpha_r\big] = \sum_{j<i} 2^{|T \cap S_j|} \cdot \big(1 + \frac{1}{\lceil l/\ln \rho \rceil}\big)^{l-r}$$

το οποίο υπολογίζεται εύκολα. ■

Η επόμενη πρόταση δίνει το κάτω φράγμα του t για τους ασθενείς σχεδιασμούς.

Πρόταση 11 *[12] Αν $S_1, ...S_m \subset [t]$ είναι ένας (m, t, l, ρ)-ασθενής σχεδιασμός, τότε*

$$t \geq \Omega(min\{\frac{l^2}{\log 2\rho}, ml\}).$$

4.3 Nisan-Wigderson generator

Συμβολισμός: Αν $S \subseteq [t]$ με $S = \{s_1, ...s_l\}$ (όπου $s_1 < s_2 < ... < s_l$) και $y \in \{0,1\}^t$, θα συμβολίζουμε με $y_{|_S} \in \{0,1\}^l$ τη συμβολοσειρά $y_{s_1} y_{s_2} ... y_{s_l}$, όπου y_{s_i} το s_i-οστό ψηφίο του y.

Ορισμός 24 *(Nisan-Wigderson generator) Έστω μια συνάρτηση* $f : \{0,1\}^l \to \{0,1\}$ *και ένας* (m,t,l,α)*-σχεδιασμός* $S = (S_1, ..., S_m)$*. Η Nisan-Wigderson γεννήτρια* $NW_{f,S} : \{0,1\}^t \to \{0,1\}^m$ *ορίζεται ως*

$$NW_{f,S}(y) = f(y_{|_{S_1}})...f(y_{|_{S_m}}).$$

Για δύο συναρτήσεις $f, g : \{0,1\}^l \to \{0,1\}$ και $0 \leq \rho \leq 1$, θα λέμε ότι η g προσεγγίζει την f σε ποσοστό ρ, αν η f και η g συμφωνούν σε ποσοστό τουλάχιστον ρ του πεδίου ορισμού τους. Ισοδύναμα $\Pr_x[f(x) = g(x)] \geq \rho$.

Λήμμα 14 *(Ανάλυση της NW γεννήτριας) Έστω ένας* (m,t,l,α)*-σχεδιασμός* S *και μία* $T : \{0,1\}^m \to \{0,1\}$*. Τότε υπάρχει μία οικογένεια* G_T *(που εξαρτάται από τα* T *και* S*) από το πολύ* $2^{m2^a+logm+2}$ *συναρτήσεις, έτσι ώστε για κάθε συνάρτηση* $f : \{0,1\}^l \to \{0,1\}$ *που ικανοποιεί*

$$|\Pr_{y\in\{0,1\}^t}[T(NW_{f,S}(y)) = 1] - \Pr_{r\in\{0,1\}^m}[T(r) = 1]| \geq \varepsilon$$

υπάρχει μία συνάρτηση $g : \{0,1\}^l \to \{0,1\}$*,* $g \in G_T$*, τ.ω. η* g *προσεγγίζει την* f *σε ποσοστό* $\frac{1}{2} + \frac{\varepsilon}{m}$*.*

ΑΠΟΔΕΙΞΗ.
$NW_{f,S}(y) = f(y_{|_{S_1}})...f(y_{|_{S_m}})$. Έστω m τυχαία bits $r_1, ..., r_m$.
Ορίζουμε τις κατανομές

$$D_i \equiv (f(y_{|_{S_1}}), f(y|_{S_2}), ..., f(y_{|_{S_i}}), r_{i+1}, ..., rm)$$

Εξ ορισμού $D_m = NW_{f,S}(y)$ και D_0 η ομοιόμορφη στο $\{0,1\}$.
• Από την υπόθεση

$$|\Pr_{y\in\{0,1\}^t}[T(NW_{f,S}(y)) = 1] - \Pr_{r\in\{0,1\}^m}[T(r) = 1]| \geq \varepsilon$$

υπάρχει ένα bit $b_0 \in \{0,1\}$ τ.ω.

$$\Pr_y[T'(NW_{f,S}(y)) = 1] - \Pr_r[T'(r) = 1] \geq \varepsilon$$

όπου $T'(x) = b_0 \oplus T(x)$, (δηλ. βγάλαμε την απόλυτη τιμή).

$$\Pr_y[T'(NW_{f,S}(y)) = 1] - \Pr_r[T'(r) = 1] =$$

$$\Pr[T'(D_m) = 1] - \Pr[T'(D_0) = 1] =$$

$$\sum_{i=1}^{m}(\Pr[T'(D_i) = 1] - \Pr[T'(D_{i-1}) = 1]) \geq \varepsilon$$

(το γράψαμε σαν σειρά).
• Άρα υπάρχει ένα i τέτοιο ώστε

$$\Pr[T'(D_i) = 1] - \Pr[T'(D_{i-1}) = 1] \geq \frac{\varepsilon}{m} \tag{4.1}$$

Επειδή η $T'(D_i)$ παίρνει τιμές στο $\{0,1\}$, παρατηρούμε ότι $\Pr[T'(D_i) = 1] = E[T'(Di)]$. Άρα

$$(4.1) \Leftrightarrow E[T'(D_i)] - E[T'(D_{i-1})] =$$

$$E[T'(Di) - T'(D_{i-1})] =$$

$$E[T'(f(y_{|S_1}), f(y_{|S_2}), ..., f(y_{|S_i}), r_{i+1}, ..., rm)$$

$$-T'(f(y_{|S_1}), f(y|S_2), ..., f(y_{|S_{i-1}}), r_i, ..., rm)] \geq \frac{\varepsilon}{m} \tag{4.2}$$

Μπορούμε να θεωρήσουμε χωρίς βλάβη της γενικότητας ότι $S_i = \{1, ..., l\}$. τότε μπορούμε να δούμε το $y \in \{0,1\}^t$ σαν ένα ζεύγος (x, z) όπου $x = y_{|S_i} \in \{0,1\}^l$ και $z = y_{|[t]-S_i} \in \{0,1\}^{t-l}$. Για κάθε $j < i$ και $y = (x, z)$ ορίζουμε $h_j(x, z) = y_{|S_i}$. (Εδώ παρατηρούμε , αλλά δεν θα χρειαστεί ακόμα, ότι το $h_j(x, z)$ εξαρτάται από $|S_i \cap S_j| \leq \alpha$ bits του x και $l - |S_i \cap S_j| \geq l - \alpha$ bits του z). Η (4.2) ξαναγράφεται

$$E_{ri,...,r_m,x,z}[T'(f(h_1(x, z)), ..., f(h_{i-1}(x, z)), f(x), r_{i+1}, ..., r_m)-$$

$$-T'(f(h_1(x, z)), ..., f(h_{i-1}(x, z)), r_i, ..., r_m)] \geq \frac{\varepsilon}{m}$$

• Αυτή είναι η μέση τιμή για όλα τα $r_i, ..., r_m, x, z$, άρα υπάρχει μία πλειάδα $(r_{i+1}, ..., r_m, z) = (c_{i+1}, ..., c_m, w)$ (δηλ. φιξάρουμε όλα εκτός από τα r_i, x) τ.ω.

$$E_{r_i,x}[T'(f(h_1(x, w)), ..., f(h_{i-1}(x, w)), f(x), c_{i+1}, ..., c_m)-$$

$$-T'(f(h_1(x, w)), ..., f(h_{i-1}(x, w)), r_i, c_{i+1}, ..., c_m)] \geq \frac{\varepsilon}{m} \tag{4.3}$$

Ορίζουμε την $F : \{0,1\}^{l+1} \to \{0,1\}^m$ ως
$F(x, b) = f(h_1(x, w)), ..., f(h_{i-1}(x, w)), b, c_{i+1}, ..., c_m)$, μετονομάζουμε το r_i σαν b και γυρίζουμε στο συμβολισμό με πιθανότητες, οπότε

$$(4.3) \Leftrightarrow \Pr_{x,b}[T'(F(x, f(x)))] = 1] - \Pr_{x,b}[T'(F(x, b)) = 1] \geq \frac{\varepsilon}{m} \tag{4.4}$$

Δηλαδή με την $T'(F(\cdot))$ μπορούμε να διακρίνουμε ένα ζεύγος $(x, f(x))$ από μία τυχαία συμβολοσειρά μήκους $l + 1$.
• Τώρα θα προσεγγίσουμε την f. Θεωρούμε την εξής διαδικασία. Για δεδομένο x διαλέγουμε ένα τυχαίο $b \in \{0,1\}$, και υπολογίζουμε το $T'(F(x, b))$. Αν

$T'(F(x,b))=1$ τότε $g_b(x)=b$ αλλιώς $g_b(x)=1-b$.
Για τα τυχαία x και b η $g_b(x)$ είναι ίση με $f(x)$ με πιθανότητα τουλάχιστον $\frac{1}{2}+\frac{\varepsilon}{m}$: ισχύει

$$\Pr_{x,b}[T'(f(x,b))=1]=$$

$$\frac{1}{2}\Pr[T'(F(x,b))=1 \mid b=f(x)]+\frac{1}{2}\Pr[T'(F(x,b))=1 \mid b\neq f(x)]$$

άρα

$$(4.4)\Rightarrow \Pr_{x,b}[T'(f(x,b))=1]=$$

$$\frac{1}{2}\Pr[T'(F(x,b))=1 \mid b=f(x)]-\frac{1}{2}\Pr[T'(F(x,b))=1 \mid b\neq f(x)]\geq \frac{\varepsilon}{m} \tag{4.5}$$

οπότε έχουμε

$$\Pr_{x,b}[g_b(x)=f(x)]=$$

$$\Pr[g_b(x)=f(x) \mid b=f(x)]\Pr[b=f(x)]+\Pr[g_b(x)\neq f(x) \mid b=f(x)]\Pr[b\neq f(x)]=$$

$$\frac{1}{2}\Pr[T'(F(x,b))=1 \mid b=f(x)]+\frac{1}{2}\Pr[T'(F(x,b))=0 \mid b\neq f(x)]=$$

$$\frac{1}{2}\Pr[T'(F(x,b))=1 \mid b=f(x)]+\frac{1}{2}-\frac{1}{2}\Pr[T'(F(x,b))=1 \mid b\neq f(x)]$$

$$\overset{(4.5)}{\geq} \frac{1}{2}+\frac{\varepsilon}{m}$$

Παίρνουμε δεσμευμένες πιθανότητες για $b=1$,$b=0$

$$\Pr_{x,b}[g_b(x)=f(x)]\geq \frac{1}{2}+\frac{\varepsilon}{m}\Leftrightarrow$$

$$\Pr_{x,b}[g_b(x)=f(x) \mid b=0]\Pr[b=0]+\Pr_{x,b}[g_b(x)=f(x) \mid b=1]\Pr[b=1]=$$

$$\Pr_x\frac{1}{2}[g_0(x)=f(x)]+\frac{1}{2}\Pr_x[g_1(x)=f(x)]\geq \frac{1}{2}+\frac{\varepsilon}{m}$$

Άρα θα πρέπει είτε $\Pr_x[g_0(x)=f(x)]\geq \frac{1}{2}+\frac{\varepsilon}{m}$ είτε $\Pr_x[g_1(x)=f(x)]\geq \frac{1}{2}+\frac{\varepsilon}{m}$, δηλ. υπάρχει ένα bit $b_1\in\{0,1\}$ τ.ω. η g_{b_1} προσεγγίζει την f σε ποσοστό $\frac{1}{2}+\frac{\varepsilon}{m}$.

Η g_{b_1} δεδομένης της T, θέλει το πολύ $2+logm+m2^a$ bits για να περιφραφεί: το b_1, το b_0 τ.ω. $T'=b_0\oplus T$, και για την F θέλουμε $logm$ bits για να προσδιορίσουμε το i, $(m-i)$ bits για τα $c_{i+1},...,c_m$, και για κάθε $j<i$ πρέπει να περιγράψουμε την $f(h_j(x,w))$. Το $h_j(x,w)$ εξαρτάται από τα $\mid S_i\cap S_j\mid\leq\alpha$ bits του x (αφού τα υπόλοιπα είναι φιξαρισμένα), δηλαδή πρέπει να προσδιορίσουμε 2^α τιμες (bits) για να περιγράψουμε την $f(h_j(x,w))$. Άρα θέλουμε άλλα $(i-1)2^\alpha$ bits . Συνολικά $2+logm+(i-1)2^\alpha+(m-1)<2+logm+m2^\alpha$ bits . ■

4.3.1 Σημείωση στο NW generator

Πριν προχωρήσουμε στον extractor του Trevisan , θα δούμε με συντομία τι είδους συνάρτηση f χρειαζόμαστε για να έχουμε ψευδοτυχαία γεννήτρια.

Ορισμός 25 *Μία κατανομή X πάνω στο $\{0,1\}^n$ λέγεται (s,ε)-ψευδοτυχαία, αν για κάθε κύκλωμα μεγέθους το πολύ s ισχύει*

$$|\Pr_{x\in X}[C(x)=1]-\Pr_{x\in U_n}[C(x)=1]|\leq\varepsilon$$

Δηλαδή ένας χρονικά περιορισμένος αντίπαλος συμπεριφέρεται με τον ίδιο τρόπο είτε παίρνει σαν είσοδο ένα εντελώς τυχαίο string , είτε ένα ψευδοτυχαίο από την X.

Ορισμός 26 *Μια οικογένεια $\{G_n\}_{n\in N}$ από συναρτήσεις $G_n:\{0,1\}^{l(n)}\rightarrow\{0,1\}^n$, λέγεται $(s,\varepsilon)-PRG$ (pseudorandom generator) εάν*

- *Η G υπολογίζεται σε χρόνο $2^{O(l(n))}$.*
- *Η κατανομή $G(U_{l(n)})$ είναι (s,ε)-ψευδοτυχαία.*

Τώρα θα ορίσουμε τι σημαίνει 'δύσκολο να προσεγγιστεί' μία συνάρτηση.

Ορισμός 27 *Μία συνάρτηση $f:\{0,1\}^n\rightarrow\{0,1\}$ θα τη λέμε (s,ε)-hard , (ή δύσκολο να προσεγγιστεί), αν για κάθε κύκλωμα μεγέθους το πολύ s ισχύει*

$$|\Pr_{x\in U_n}[C(x)=f(x)]-\frac{1}{2}|\leq\varepsilon$$

Δηλαδή κάθε κύκλωμα C μεγέθους το πολύ s υπολογίζει σωστά την f σε περίπου τα μισά σημεία του πεδίου ορισμού της. Ή ισοδύναμα κανένα κύκλωμα C μεγέθους το πολύ s δεν μπορεί να κάνει κάτι καλύτερο από το να μαντέψει στην τύχη το $f(x)$, που σημαίνει ότι η f για το C φαίνεται τυχαία.

Οπότε για να έχουμε ότι η $NW_{f,S}(y)$ είναι (s,ε)-ψευδοτυχαία γεννήτρια, θα πρέπει να ισχύει για κάθε T που υπολογίζεται από κύκλωμα μεγέθους το πολύ s

$$|\Pr_{y\in\{0,1\}^t}[T(NW_{f,S}(y))=1]-\Pr_{r\in\{0,1\}^m}[T(r)=1]\geq\varepsilon$$

που αυτό αποδείξαμε ότι συνεπάγεται ότι υπάρχει μία οικογένεια G_T και μία συνάρτηση $g\in G_T$ που προσεγγίζει την f σε ποσοστό $\frac{1}{2}+\frac{\varepsilon}{m}$, δηλαδή

$$\Pr_{x\in U_l}[g(x)=f(x)]\geq\frac{1}{2}+\frac{\varepsilon}{m}$$

Παρατηρούμε, όμως, επιπλέον, ότι το $g(x)$ για να υπολογιστεί χρειάζεται να υπολογίσει το $T'(F(x,b))$, άρα χρειάζεται κύκλωμα μεγέθους s για την T', και κύκλωμα μεγέθους το πολύ $m2^\alpha$ για την F, (αφού η F έχει υπολογισμό το πολύ m boolean συναρτήσεων $f(h_i(x,w))$, που είναι (το πολύ) α μεταβλητών η καθεμία.

Πόρισμα 2 *Αν η συνάρτηση f είναι $(s+m2^\alpha, \frac{\varepsilon}{m})$-hard , τότε η $NW_{f,S}(y)$ είναι (s,ε)-PRG.*

Πόρισμα 3 *Αν η συνάρτηση f είναι $(2n^2, \frac{1}{n^2})$-hard , τότε η $NW_{f,S}(y)$ είναι $(n^2, \frac{1}{n})$-PRG.*

4.4 Trevisan's Extractor

Ορισμός 28 *(Trevisan's Extractor) Έστω ένας κώδικας διόρθωσης λαθών $C : \{0,1\}^n \to \{0,1\}^{\overline{n}}$, όπως στο λήμμα 9, με $\delta = \frac{\varepsilon}{m}$, $\overline{n} = poly(n, \frac{1}{\varepsilon})$.*
Έστω ένας (m,t,l,α)-σχεδιασμός S όπως στο λήμμα 10, με $l = log\overline{n} = O(logn/\varepsilon)$.
Ορίζουμε τον extractor $Ext : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ ως

$$Ext(x,y) = C(x)_{y_1} C(x)_{y_2} ... C(x)_{y_m}$$

όπου $y_i = y_{|S_i}$, δηλ. το $C(x)_{y_i}$ είναι το y_i-οστό ψηφίο του $C(x)$.

Θα υπολογίσουμε τις παραμέτρους ώστε ο Ext να είναι $(k, 2\varepsilon)$-extractor :

Έστω μία πηγή X με ελάχιστη εντροπία k.

Θέλουμε (από τον ορισμό του extractor) η στατιστική απόσταση του $Ext(X,U_t)$ από την U_m να είναι το πολύ 2ε.

$$\Delta(E(X,U_t), U_m) \leq 2\varepsilon \Leftrightarrow$$

$$\max_T \mid \Pr[T(Ext(X,U_t)) = 1] - \Pr[T(U_m) = 1] \mid \leq 2\varepsilon$$

Πρέπει για κάθε $T : \{0,1\}^m \to \{0,1\}$ να ισχύει

$$\mid \Pr[T(Ext(X,U_t)) = 1] - \Pr[T(U_m) = 1] \mid \leq 2\varepsilon$$

Έστω B το σύνολο των $x \in X$ για τα οποία

$$\mid \Pr[T(Ext(x,U_t)) = 1] - \Pr[T(U_m) = 1] \mid \geq \varepsilon$$

Αρκεί το B να είναι μικρό, για την ακρίβεια αρκεί $\Pr[X \in B] \leq \varepsilon$, γιατί τότε έχω

$$\begin{aligned}
&| \Pr[T(Ext(X,Ut)) = 1] - \Pr[T(U_m) = 1] | = \\
&| E_{x \in X}[Pr[T(Ext(x,U_t)) = 1] - \Pr[T(U_m) = 1]] | \leq \\
&E_{x \in X}[| \Pr[T(Ext(x,Ut)) = 1] - \Pr[T(U_m) = 1] |] = \\
&\sum_{x \in B} \Pr[X = x] \mid \Pr[T(Ext(x,Ut)) = 1] - \Pr[T(U_m) = 1] \mid + \\
&+ \sum_{x \notin B} \Pr[X = x] \mid \Pr[T(Ext(x,Ut)) = 1] - \Pr[T(U_m) = 1] \mid \leq \\
&\varepsilon \cdot 1 + 1 \cdot \varepsilon \leq 2\varepsilon
\end{aligned}$$

Άρα αρκεί $|B| \leq \varepsilon \cdot 2^k$ (ώστε $\Pr[X \in B] = \frac{|B|}{|X|} \leq \frac{|B|}{2^k} \leq \varepsilon$).

Για δεδομένο T, θα υπολογίσουμε το $|B|$:

Από το λήμμα 14 έχω ότι για κάθε $f : \{0,1\}^l \to \{0,1\}$ τέτοια ώστε $| \Pr_{y \in U_t}[T(NW_{f,S}(y)) = 1] - \Pr_{r \in U_m}[T(r) = 1] | \geq \varepsilon$, υπάρχει μία $g : \{0,1\}^l \to \{0,1\}$ που προσεγγίζει την f σε ποσοστό $\frac{1}{2} + \frac{\varepsilon}{m}$, και έχει μήκος αναπαράστασης $m2^\alpha + logm + 2$.

Αν θεωρήσουμε το $C(x)$ σαν την αναπαράσταση μιας συνάρτησης f, (δηλαδή το $C(x)$ να είναι η παράθεση των τιμών $f(1)f(2)...f(\overline{n})$) τότε από το λήμμα 4.1 έχουμε ότι για κάθε $x \in X$, δηλ. $\forall x \in B$, τ.ω. $| \Pr[T(Ext(x,U_t)) = 1] - \Pr[T(U_m) = 1] | > \varepsilon$ υπάρχει μία g με μήκος αναπαράστασης $m2^\alpha + logm + 2$ bits , που προσεγγίζει την f σε ποσοστό $\frac{1}{2} + \frac{\varepsilon}{m}$. Ισοδύναμα υπάρχει μία συμβολοσειρά μήκους $m2^\alpha + logm + 2$ που έχει απόσταση Hamming μικρότερη από $(\frac{1}{2} - \frac{\varepsilon}{m})\overline{n}$ από το $C(x)$.

Το πλήθος των δυνατών g είναι $2^{m2^\alpha + logm + 2}$, αλλά κάθε g μπορεί να προσεγγίσει το πολύ $(\frac{m}{\varepsilon})^2$ συμβολοσειρές $C(x)$, επειδή ο C είναι κώδικας διόρθωσης λαθών τ.ω. κάθε Hamming σφαίρα ακτίνας $(\frac{1}{2} - \delta)$ έχει το πολύ $\frac{1}{\delta^2}$ στοιχεία.

Άρα το $|B|$ μπορεί να είναι το πολύ ίσο με $2^{m2^\alpha + logm + 2} \cdot (\frac{m}{\varepsilon})^2$.

Επομενως για να έχω $(k, 2\varepsilon)$-extractor αρκεί $|B| \leq \varepsilon \cdot 2^k \Leftrightarrow$

$$2^{m2^\alpha + logm + 2} \cdot (\frac{m}{\varepsilon})^2 \leq \varepsilon \cdot 2^k \Leftrightarrow$$

$$m2^\alpha + 3logm + 2 + 3log(1/\varepsilon) \leq k \tag{4.6}$$

Θεώρημα 29 *Αν* $k \leq n$, $36 \leq m \leq k/2$, $0 < \varepsilon < 2^{\frac{-k}{12}}$ *και* $\alpha = log(\frac{k}{2m})$, *τότε η συνάρτηση Ext όπως την ορίσαμε στον ορισμό 28, είναι* $(k, 2\varepsilon)$*-extractor .*

ΑΠΟΔΕΙΞΗ. Η παραπάνω επιλογή παραμέτρων ικανοποιεί την 4.6. ■

Σημείωση Τα τυχαία bits που χρειαζόμαστε είναι από την κατασκευή του σχεδιασμού $t = O(e^{\frac{lnm}{log(k/2m)}} \frac{(log\overline{n})^2}{log(k/2m)})$.

4.4.1 Trevisan's Extractor is Strong

Μπορούμε να αποδείξουμε ότι ο Ext όπως τον ορίσαμε στον ορισμό 28 είναι strong-extractor , τροποποιώντας την απόδειξη, με τις εξής διαφορές.

Αντί να χρησιμοποιήσουμε distinguisher, χρησιμοποιούμε next bit predictor, δηλαδή αντί να χρησιμοποιήσουμε ότι $\Delta(X,Y) > \varepsilon \Leftrightarrow$ υπάρχει (distinguisher) $T : \{0,1\}^m \to \{0,1\}$ τ.ω. $\mid \Pr[T(X) = 1] - \Pr[T(Y) = 1] \mid > \varepsilon$, θα χρησιμοποιήσουμε το λήμμα του Yao [19] που λέει $\Delta((Y,Z),(U_t \times U_m)) > \varepsilon$, $U \sim U_m \Leftrightarrow$ υπάρχει $i \in [m]$ και (next bit predictor) $A : \{0,1\}^t \times \{0,1\}^{i-1} \to \{0,1\}$ τ.ω. $\Pr_{y,z}[A(y, z_1 z_2 ... z_{i-1}) = z_i] > \frac{1}{2} + \frac{\varepsilon}{m}$.

Επιπλέον αντί για το λήμμα 14 (της NW γεννήτριας), χρησιμοποιούμε το εξής λήμμα.

Λήμμα 15 *Έστω σχεδιασμός* S *με* $|S_i \cap S_j| \leq \alpha$. *Για κάθε* $i \in [m]$ *υπάρχει ένα σύνολο* H_i *από συναρτήσεις* $h : \{0,1\}^l \to \{0,1\}^{t+i-1}$ *(που εξαρτάται από το* S *και το* i*) τ.ω.*

1. *Για κάθε συνάρτηση* $f : \{0,1\}^l \to \{0,1\}$ *και κάθε predictor* $A : \{0,1\}^{t+i-1} \to \{0,1\}$ *υπάρχει μία* $h \in H_i$ *τ.ω.*

$$\Pr_x[A(h(x)) = f(x)] \geq \Pr_y[A(y, f(y_{|S_1}) ... f(y_{|S_{i-1}})) = f(y_{|S_i})]$$

   όπου το x *επιλέγεται ομοιόμορφα από το* $\{0,1\}^l$ *και το* y *από το* $\{0,1\}^t$.

2. $log \mid H_i \mid \leq t + \sum_{j<i} 2^{|S_i \cap S_j|} \leq t + m2^\alpha$

ΑΠΟΔΕΙΞΗ. Έστω $\Pr_y[A(y, f(y_{|S_1}) ... f(y_{|S_{i-1}})) = f(y_{|S_i})] \geq \rho$

1. Θέτουμε $x = y_{|S_i}$ και $z = y_{|[t]-S_j}$. Αν φιξάρουμε το z, τότε (προφανώς) $x \sim U_l$, και επίσης παρατηρούμε ότι το $f(y_{|S_j)}$ για $j \neq i$, είναι μια συνάρτηση του x που εξαρτάται μόνο από τα $\mid S_i \cap S_j \mid$ bits του x (αφού τα υπόλοιπα bits του $y_{|S_j}$ είναι φιξαρισμένα).
Θεωρώντας δεσμευμένες πιθανότητες ως προς όλα τα z, υπάρχει ένα $z = w$ (δηλαδή φιξάρουμε το z στην τιμή w) τ.ω.

$$\Pr_x[A(y(x), f_1(x)...f_{i-1}(x)) = f(x)] \geq \rho$$

όπου η $y(x)$ είναι το y με το x στις θέσεις που δείχνει το S_i και το w στις υπόλοιπες, και το $f_j(x)$ είναι το $f(y_{S_j})$ μετά το φιξάρισμα $z = w$.
Θέτω $H(x) = (y(x), f_1(x)...f_{i-1}(x))$.

2. Η h θέλει το πολύ $t - l < t$ bits για την περιγραφή του $y(x)$, και το πολύ $2^{|S_i \cap S_j|}$ bits για την περιγραφή κάθε $f_j(x)$. Συνολικά το πολύ $t + m2^\alpha$ bits .

■

Παρατήρηση Ορίζουμε $g : \{0,1\}^l \to \{0,1\}$ ως $g(x) = A(h(x))$. Η g προσεγγίζει την f σε ποσοστό ρ, και δεδομένης της A θέλει $t + m2^\alpha$ bits για να περιγραφτεί. Ορίζουμε G_A την οικογένεια που περιλαμβάνει όλες τις g που περιγράφονται με αυτόν τον τρόπο.

Επομένως το λήμμα 15, για κάθε next bit predictor A και για δεδομένα S (σχεδιασμός) και $i \in [m]$, μας δίνει μια οικογένεια G_A από 2^{t+m2^α} συναρτήσεις, τέτοια ώστε για κάθε $f : \{0,1\}^l \to \{0,1\}$ τ.ω. $\Pr_y[A(y, f(y_{|S_1})...f(y_{|S_{i-1}})) = f(y_{|S_i})] \geq \rho$, υπάρχει μία $g \in G_A$, $g : \{0,1\}^l \to \{0,1\}$ που προσεγγίζει την f σε ποσοστό ρ.

Η υπόλοιπη απόδειξη είναι ίδια, δηλαδή:

Έστω X κατανομή με ελάχιστη εντροπία k.

Για να έχουμε (k, ε)-strong extractor πρέπει $\Delta(U_t \times Ext(X, U_t), U_t \times U_m) \leq \varepsilon$. Από το λήμμα του Yao [19] αρκεί για κάθε $A : \{0,1\}^t \times \{0,1\}^{i-1} \to \{0,1\}$ να ισχύει

$$\Pr_{\substack{x \sim X \\ y \sim U_t}}[A(y, C(x)_{y_1}...C(x)_{y_{i-1}}) = C(x)_{y_i}] \leq \frac{1}{2} + \frac{\varepsilon}{m}$$

Έστω A. Άστω B το σύνολο των $X \in X$ για τα οποία

$$\Pr_y[A(y, C(x)_{y_1}...C(x)_{y_{i-1}}) = C(x)_{y_i}] > \frac{1}{2} + \frac{\varepsilon}{m}$$

Αρκεί $\Pr[X \in B] \leq \frac{|B|}{2^k} \leq \frac{\varepsilon}{2m}$ γιατί τότε έχουμε

$$\begin{aligned}
\Pr_{x,y}[A(y, C(x)_{y_1}...C(x)_{y_{i-1}}) = C(x)_{y_i}] = \\
\Pr[x \in B] \cdot \Pr_y[A(y, C(x)_{y_1}...C(x)_{y_{i-1}}) = C(x)_{y_i} \mid x \in B] + \\
+ \Pr[x \notin B] \cdot \Pr_y[A(y, C(x)_{y_1}...C(x)_{y_{i-1}}) = C(x)_{y_i} \mid x \notin B] \leq \\
\frac{\varepsilon}{2m} \cdot 1 + 1 \cdot (\frac{1}{2} + \frac{\varepsilon}{2m}) = \\
\frac{1}{2} + \frac{\varepsilon}{m}
\end{aligned}$$

Άρα αρκεί $\mid B \mid \leq \frac{\varepsilon}{2m} 2^k$.
Για δεδομένο A θα υπολογίσουμε το $|B|$.

Θεωρούμε το $C(x)$ σαν αναπαράσταση (παράθεση των τιμών $f_1...f_m$) μιας boolean συνάρτησης F. Από το λήμμα 15 υπάρχει μία οικογένεια G_A τέτοια ώστε για κάθε $x \in B$ υπάρχει μία $g \in G_A$ που προσεγγίζει την f σε ποσοστό $\frac{1}{2} + \frac{\varepsilon}{2m}$. Ισοδύναμα, θεωρώντας τη συμβολοσειρά $g_1...g_m$, μπορούμε να πούμε ότι για κάθε $x \in B$ υπάρχει μία συμβολοσειρά που έχει απόσταση Hamming από το $C(x)$ το πολύ $\frac{1}{2} - \frac{\varepsilon}{2m}$. Το πλήθος των g είναι $|G_A| = 2^{t+m2^\alpha}$ και κάθε g μπορεί να προσεγγίσει το πολύ $(\frac{2m}{\varepsilon})^2$ συμβολοσειρές $C(x)$, λόγω της ιδιότητας του κώδικα διόρθωσης λαθών.
Άρα $|B| \leq (\frac{2m}{\varepsilon})^2 \cdot 2^{t+m2^\alpha}$.
Άρα για να έχουμε (k, ε)-strong extractor αρκεί

$$(\frac{2m}{\varepsilon})^2 \cdot 2^{t+m2^\alpha} \leq \frac{\varepsilon}{2m} 2^k \tag{4.7}$$

Διαλέγουμε τις παραμέτρους κατάλληλα.

Παρατήρηση Η διαφορά στις παραμέτρους του strong από τον απλό extractor , είναι ότι στον απλό θέλουμε $k > m2^\alpha + O(\log(\frac{m}{\varepsilon}))$,ενώ στον strong θέλουμε $k > t + m2^\alpha + O(\log(\frac{m}{\varepsilon}))$.

4.4.2 Trevisan's Extractor με ασθενείς σχεδιασμούς

Παρατηρούμε ότι στην απόδειξη του Trvisan's extractor ότι στον υπολογισμό του μεγέθους της οικογένειας G_A, το $m2^\alpha$ προκύπτει από το ότι χρειαζόμαστε $2^{|S_i \cap S_j|}$ bits για την περιγραφή κάθε $f_j(x), \forall j < i$.

Αυτό είναι ίσο με $\sum_{j<i} 2^{|S_i \cap S_j|}$. Οπότε θα μπορούσαμε να χρησιμοποιήσουμε αντί για έναν κανονικό σχεδιασμό, έναν ασθενή σχεδιασμό για τον οποίο (εξ ορισμού) ισχύει $\sum_{j<i} 2^{|S_i \cap S_j|} \leq \rho(m-1)$.

Τότε για να έχουμε strong $(k, \varepsilon)-$extractor , αρκεί να ισχύει η εξής ανισότητα

$$(\frac{2m}{\varepsilon})^2 \cdot 2^{t+\rho m} \leq \frac{\varepsilon}{2m} 2^k$$

$$\Leftrightarrow \rho m \leq k - 3\log(\frac{2m}{\varepsilon}) - t.$$

Μια βασική διαφορά του extractor που χρησιμοποιεί ασθενή σχεδιασμό αντί για απλό, είναι ότι το μέγεθος του seed (που είναι ίσο με το t του σχεδιασμού) μειώνεται από $O(m^{1/\alpha} \cdot l^2/\alpha) = O(m^{1/\log\rho} \cdot l^2/\log\rho)$ σε $O(l^2/\ln\rho)$.

Δηλαδή δεν έξαρτάται από το m.

Αναφορές. Για σχεδιασμούς [12] [17]. Για κώδικες διόρθωσης λαθών [7] [18]. Ο next bit predictor (λήμμα του Yao) [19]. Ο Nisan Wigderson generator [9]. Ο Trevisan's extractor [17]. Ο Trevisan's extractor με weak designs [12].

Κεφάλαιο 5

Εφαρμογές στην Κρυπτογραφία

Οι randomness extractors αποδεικνύονται χρήσιμοι στην κρυπτογραφία δημοσίου κλειδιού, όταν αυτή βασίζεται σε μυστικά που δεν είναι εντελώς τυχαία, δηλαδή η πηγή από την οποία προέρχονται δεν ακολουθεί την ομοιόμορφη κατανομή, αλλά έχει κάποια ελάχιστη εντροπία (k bits). Σε αυτή την περίπτωση η εντροπία εκφράζει το μέγεθος της αβεβαιότητας που έχει ένας αντίπαλος για το μυστικό W.

Το θεμελιώδες πρόβλημα της κρυπτογραφίας συμμετρικού κλειδιού είναι το εξής. Η Αλίκη και ο Βασίλης μοιράζονται ένα κοινό μυστικό W και θέλουν να επικοινωνήσουν με ασφάλεια μέσω ενός δημοσίου καναλιού, που όμως ελέγχεται από έναν ενεργό αντίπαλο (την Εύα). Η επικοινωνία τους θέλουν να είναι προσωπική και αυθεντική (να είναι σίγουροι δηλαδή ότι μιλάνε μεταξύ τους και όχι με κάποιον άλλο). Αυτό το πρόβλημα λύνεται χρησιμοποιώντας βασικά κρυπτογραφικά εργαλεία, τα οποία όμως απαιτούν το μυστικό W να είναι ομοιόμορφα κατανεμημένο.

Στην πράξη είναι γενικά δύσκολο να έχει κάποιος στη διάθεσή του εντελώς τυχαία μυστικά, γιατί είτε οι φυσικές πηγές τυχαιότητας δεν είναι είναι ομοιόμορφες, όπως π.χ. τα βιομετρικά ή οι συνθηματικές λέξεις, είτε ο αντίπαλος έχει κάποια παράπλευρη πληροφορία σχετική με το μυστικό. Εδώ φαίνεται η χρησιμότητα των randomness extractors, γιατί η Αλίκη και ο Βασίλης μπορούν να μοιράζονται ένα τέτοιο ασθενές μυστικό W, και χρησιμοποιώντας έναν extractor να το μετατρέψουν σε ένα άλλο R ομοιόμορφα κατανεμημένο. Η μόνη απάιτηση για να μπορεί να γίνει αυτό, είναι το αρχικό μυστικό W να έχει τουλάχιστον k bits εντροπίας.

Επιπλέον, όμως, παρουσιάζεται το εξής πρόβλημα. Ο extractor που χρησιμοποιείται, χρησιμοποιεί ένα τυχαίο seed y, το οποίο γίνεται δημοσίως γνωστό και άρα γνωστό και στην Εύα. Εάν ο extractor είναι strong, τότε το αποτέ-

λεσμα του extractor $R = Ext(W, y)$ είναι ομοιόμορφα κατανεμημένο, ακόμα και αν το seed είναι γνωστό. Τι γίνεται, όμως, αν η Εύα βλέποντας το seed y το αλλάξει σε y' της επιλογής της, και καταφέρει να μάθει το αποτέλεσμα του extractor για αυτό το seed, δηλ. το $R' = Ext(W, y')$. Θα θέλαμε, για κάθε επιλογή y' της Εύας, τα R και R' να μην σχετίζονται καθόλου. Εάν ο extractor έχει αυτήν την ιδιότητα, τότε τον ορίζουμε ως non-malleable extractor.

Αποδεικνύεται ότι τέτοιοι extractors υπάρχουν. Η απόδειξη όμως χρησιμοποιεί την πιθανοτική μέθοδο, και δεν είναι κατασκευαστική. Μέχρι τώρα δεν έχουμε explicit κατασκευή ενός non-malleable extractor. Μια ασθενέστερη έννοια που θα μπορούσαμε να ορίσουμε είναι αυτή του weak-non-malleable extractor, και ίσως να είναι ευκολότερο να βρούμε μία συνάρτηση με αυτήν την ιδιότητα. Weak non-malleable ορίζουμε να λέγεται ένας extractor αν για κάθε επιλογή y' του αντιπάλου, το R δεδομένου του R' έχει ακόμα κάποια ελάχιστη εντροπία (αν ακι μικρότερη από αυτήν που θα είχε αν ήταν non malleable).

5.1 Πιστοποίηση γνησιότητας μηνύματος

Το πρόβλημα της πιστοποίησης γνησιότητας μηνύματος (message authentication) είνια το εξής. Η Αλίκη και ο Βασίλης μοιράζονται ένα μυστικό W από μία μη ομοιόμορφη πηγή, για το οποίο η Εύα έχει κάποια παράπλευρη πληροφορία Z. Η Αλίκη θέλει να στείλει στον Βασίλη ένα μήνυμα μ_A μαζί με μία απόδειξη γνησιότητας (απόδειξη ότι προέρχεται από αυτήν), με την Εύα να είναι ενεργός αντίπαλος και να μπορεί να τροποποιήσει τα μηνύματα που στέλνονται με όποιον τρόπο θέλει. Ο Βασίλης θα πρέπει είτε να λάβει σωστά το μ_A, είτε να αντιληφθεί ενεργή επίθεση και να τερματίσει βγάζοντας $\perp$.

Ορισμός 30 *Ένα (n, k, m, δ)-message authentication πρωτόκολλο, είναι ένα πρωτόκολλο στο οποίο η Αλίκη ξεκινάει με ένα αρχικό μύνημα $\mu_A \in \{0,1\}^m$, και στην κατάληξη του πρωτοκόλλου ο Βασίλης βγάζει σαν αποτέλεσμα ένα παραληφθέν μήνυμα $\mu_B \in \{0,1\}^m \cup \{\perp\}$. Απαιτούνται οι εξής ιδιότητες.*

Ορθότητα. Αν ο αντίπαλος είναι παθητικός (passive) τότε για κάθε αρχικό μήνυμα $\mu_A \in \{0,1\}^m$, $\Pr[\mu_B = \mu_A] = 1$.

Ασφάλεια. Αν $(W|Z)$ είναι μία (n,k)-source,τότε για κάθε αρχικό μήνυμα $\mu_A \in \{0,1\}^m$ και για οποιαδήποτε ενεργή στρηγική αντιπάλου, $\Pr[\mu_B \notin \{\mu_A, \perp\}] \leq \delta$.

Για εντελώς τυχαία μυστικά W το πρόβλημα λύνεται χρησιμοποιώντας message authentication codes (MAC).

Ορισμός 31 *Μία οικογένεια συναρτήσεων $\{MAC_r : \{0,1\}^m \to \{0,1\}^s\}_{r \in \{0,1\}^n}$ είναι δ-ασφαλής message authentication code (MAC) αν για κάθε $\mu \neq \mu', \sigma, \sigma'$,*

$\Pr[MAC_R(\mu) = \sigma | MAC_R(\mu') = \sigma'] \leq \delta$ *όπου το* R *είναι ομοιόμορφο πάνω στο* $\{0,1\}^n$.

Δηλαδή η Αλίκη στέλνει το μήνυμά της μ_A μαζί με μία ετικέτα (αναγνωριστική ένδειξη) $\sigma = MAC_W(\mu_A)$ την οποία υπολογίζει με βάση το κοινό μυστικό W. Ο Βασίλης θα αποδεχτεί το μήνυμα που θα λάβει (μ_B) αν $MAC_W(\mu_B) = \sigma = MAC_W(\mu_A)$.

Αυτό το πρωτόκολλο αποδεικνύεται ότι δεν λειτουργεί για μη εντελώς τυχαία μυστικά. Αυτό το πρόβλημα μπορέι να αντιμετωπιστεί χρησιμοποιώντας έναν strong extractor, που θα μετατρέψει το μη ομοιόμορφο μυστικό σε ομοιόμορφο, και το πρωτόκολλο πιστοποίησης θα είναι ως εξής.

Ο Βασίλης στέλνει στην Αλίκη ένα seed X το οποίο επιλέγει τυχαία. Η Αλίκη και ο Βασίλης υπολογίζουν το $R = Ext(W, X)$ όπου Ext ένας strong extractor. Η Αλίκη στέλνει το μήνυμά της μ_A μαζί με την ετικέτα $\sigma = MAC_R(\mu_A)$. Ο Βασίλης αποδέχεται το μύνημα που λαμβάνει (μ_B) αν $MAC_R(\mu_B) = \sigma$.

Το πρόβλημα τώρα είναι το εξής. Η Εύα βλέποντας το W μπορεί να το αλλάξει σε X' της επιλογής της και να το στείλει στην Αλίκη. Μετά η Αλίκη υπολογίζει το $R' = Ext(W, X')$ και το $\sigma' = MAC_{R'}(\mu_A)$ και στέλνει (μ_A, σ'). Η Εύα βλέποντας το (μ_A, σ') είναι δυνατόν να επιτύχει επίθεση σχετιζομένου κλειδιού και να βρει μία αποδεκτή ετικέτα $\tilde{\sigma}$ για ένα δικό της μήνυμα μ_B (δηλ. $\tilde{\sigma} = MAC_R(\mu_B)$ με το πραγματικό R) και να στείλει στον Βασίλη $(\mu_b, \tilde{\sigma})$. Έτσι ο Βασίλης θα αποδεχθεί το μ_B σαν να προερχόταν από την Αλίκη (βλ.σχήμα 1).

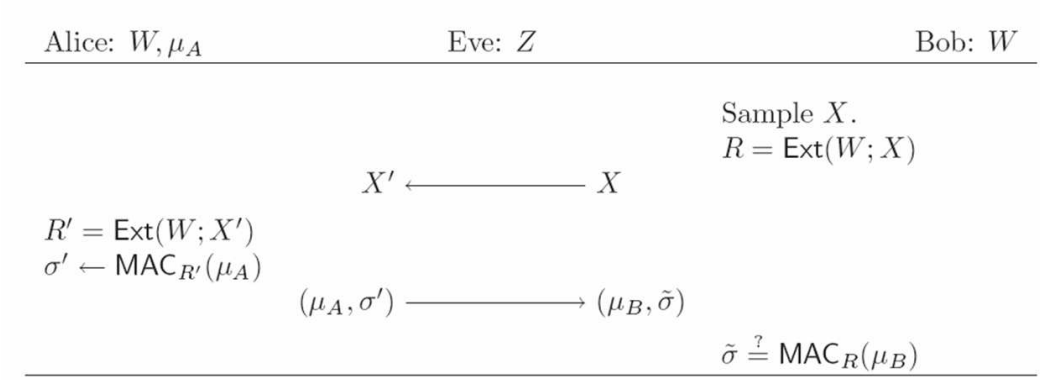


Figure 1: A Framework for Message Authentication Protocols.

Ένας τρόπος για να μην μπορεί να γίνει η επίθεση σχετιζομένου κλειδιού, είναι για οποιαδηποτε επιλογή του X' από την Εύα, τα R, R' να μην σχετίζονται. Ορίζουμε έναν extractor να λέγεται non malleable , αν έχει αυτήν την ιδιότητα.

Αποδεικνύεται ότι υπάρχει non malleable extractor, αλλά μέχρι τώρα δεν έχει κατασκευαστεί.

5.2 Non Malleable Extractors

Θεωρούμε την εξής επίθεση για την ιδιότητα της non-malleability. Ο αντίπαλος βλέπει το seed x και το μετατρέπει σε X'. Μετά μαθαίνει την τιμή R' του extractor με seed X' και μυστικό W (το οποίο δεν γνωρίζει). Θέλουμε το (σωστό) R να είναι ομοιόμορφα τυχαίο, ακόμα και με δεδομένο το R', οπότε τα R, R' θα είναι τελείως άσχετα μεταξύ τους.

Ορισμός 32 *Λέμε οτι μία συνάρτηση* $Ext : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *είναι* (n,k,d,m,ϵ) *non malleable extractor,αν για κάθε k-source* W*, και για κάθε συνάρτηση αντιπάλου* $A : \{0,1\}^d \to \{0,1\}^d$*, έχουμε*

$$(X, Ext(W, A(X)), Ext(W, X)) \sim_\epsilon (X, Ext(W, A(X)), U_m)$$

όπου το X (seed) είναι ομοιόμορφα κατανεμημένο στο $\{0,1\}^d$ *και* $A(X) \neq X$*.*

Θεώρημα 33 *Υπάρχει* (n,k,d,m,ϵ) *non malleable extractor,αν*

$$d > \log(n-k+1) + 2\log(1/\epsilon) + 5 \tag{5.1}$$

$$k > 2m + 2\log(1/\epsilon) + \log(d) + 6 \tag{5.2}$$

ΑΠΟΔΕΙΞΗ. Θα αποδείξουμε το θεώρημα με την πιθανοτική μέθοδο, δείχνοντας ότι μία τυχαία συνάρτηση R είναι non malleable extractor με μεγάλη πιθανότητα. Κατ' αρχάς μία συνάρτηση $R : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ είναι (n,k,d,m,ϵ) non malleable extractor,αν για κάθε distinguisher $T : \{0,1\}^d \times \{0,1\}^m\{0,1\}^m \to \{0,1\}$, κάθε συνάρτηση αντιπάλου A και κάθε k-source W:

$$\Pr[T(X, R(W, A(X)), R(W, X)) = 1] - \Pr[T(X, R(W, A(X)), U_l) = 1] \leq \varepsilon \tag{5.3}$$

Επιπλέον αρκεί να θεωρήσουμε μόνο τις flat k-sources, γιατί αν η (5.9) αποτυγχάνει για μια οποιαδήποτε k-source W, τότε υπάρχει μια flat k-source για την οποία αποτυγχάνει.

Φιξάρουμε τα T, A, W. Θα συμβολίζουμε με R την τυχαία μεταβλητή που είναι ομοιόμορφα κατανεμημένη στο χώρο όλων των συναρτήσεων $R : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$.

Για κάθε $x \in \{0,1\}^d, u \in \{0,1\}^m$, ορίζουμε

$$Count(x,u) := |\{u_2 \in \{0,1\}^m \ : \ T(x,u,u_2) = 1\}| \tag{5.4}$$

Για κάθε $w \in W$, $x \in \{0,1\}^d$ όρίζουμε τις εξής τυχαίες μεταβλητές, (που παίρνουν την τυχαιότητά τους από την R):

$$Left(w,x) := T(x, R(w, A(x)), R(w,x)) \tag{5.5}$$

$$Right(w,x) := \left(\frac{Count(x, R(w, A(x)))}{2^m}\right) \tag{5.6}$$

$$Q(w,x) := Left(w,x) - Right(w,x) \tag{5.7}$$

$$\bar{Q}(w,x) := \frac{\sum w, xQ(w,x)}{2^{k+d}} \tag{5.8}$$

Ουσιαστικά η $\bar{Q}$ είναι μία τυχαία μεταβλητή που αντιστοιχεί κάθε σε κάθε R την τιμή

$$p(R) := \Pr[T(X, R(W, A(X)), R(W,X)) = 1] - \Pr[T(X, R(W, A(X)), U_l) = 1] \tag{5.9}$$

Οπότε θέλουμε να φράξουμε από πάνω την πιθανότητα

$$\Pr[\bar{Q} > \varepsilon] = \Pr_R[p(R)] > \varepsilon \tag{5.10}$$

Παρατηρούμε ότι για κάθε w, x έχουμε $E[Left(w,x)] = E[Right(w,x)]$ και έτσι $E[Q(w,x)] = 0$ και $E[\bar{Q}] = 0$. Παρ'ολα αυτά οι τιμές $Q(w,x)$ δεν είναι οπωσδήποτε ανεξάρτητες μεταξύ τους οπότε δεν μπορούμε να χρησιμοποιήσουμε ένα Chernoff Bound στην 5.10. Για παράδειγμα αν $A(A(x))$ τότε τα

$$Left(w,x) = T(x, R(w, A(x)), R(w,x))$$

και

$$Left(w, A(x)) = T(A(x), R(w,x), R(w, A(x)))$$

δεν είναι ανεξάρτητα και έτσι δεν είναι ανεξάρτητα και τα $Q(w,x), Q(w, A(x))$. Θα δείξουμε ότι όλη η κακή εξάρτηση είναι ουσιαστικά αυτής της μορφής. Πιο συγκεκριμένα ας αναπαραστήσουμε τη συνάρτηση A σαν ένα κατευθυνόμενο γράφημα $G = (V, E)$ πάνω στο σύνολο των κορυφών $V = \{0,1\}^d$ και με ακμές $E := \{(A(x), x) : x \in \{0,1\}^d\}$ δηλαδή υπάρχει μία ακμή από το x' στο x ανν $A(x) = x'$. Αφού η A είναι συνάρτηση το πλήθος των εισερχόμενων ακμών σε κάθε κορυφή είναι 1. Θα δείξουμε ότι αν περιοριστούμε σε τιμές του x που περιέχονται σε ένα υποσύνολο του V που δεν περιέχει κύκλους, τότε οι μεταβλητές $Q(x,w)$ μπορεί να έχουν πολύ περιορισμένη εξάρτηση.

Λήμμα 16 *Για $V' \subseteq V$ έστω $G' \subseteq G$ ο περιορισμός του G στις ακμές V' και ας υποθέσουμε ότι το γράφημα G' είναι ένα ακυκλικό υπογράφημα του G. Τότε το σύνολο $\{Q(w,x)\}_{w \in W, x \in V'}$ από τυχαίες μεταβλητές μπορεί να αριθμηθεί ως $Q_1, ..., Q_l$ για $l = |V'|2^k$ τέτοιο ώστε $E[Q_i | Q_1, ..., Q_{i-1}]$ για κάθε $1 \leq i \leq l$.*

ΑΠΟΔΕΙΞΗ. Το γράφημα G' είναι ένα κατευθυνόμενο κυκλικό γράφημα και έτσι ορίζει μια μερική διάταξη $' \leq'$ πάνω στις κορυφές V' έτσι ώστε αν $(x', x) \in E'$ τότε $x' \leq x$. Χρησιμοποιούμε τη μερική διάταξη πάνω στο V' για να ορίσουμε μια μερική διάταξη πάνω στο σύνολο $\{Q(w,x)\}_{w\in W, x\in V'}$. Τέλος μπορούμε να επεκτείνουμε αυτή τη μερική διάταξη σε μία ολική διάταξη και έτσι να αριθμήσουμε το παραπάνω σύνολο ως $Q_1, ..., Q_l$ έτσι ώστε αν $x' \leq x$ και $Q_i = Q(w, x'), Q_j = Q(w, x)$ τότε $i \leq j$. Τώρα δείχνουμε ότι για κάθε $1 \leq i \leq l$ έχουμε $E[Q_i|Q_1, ..., Q_{i-1}]$. Η τυχαιότητα αυτών των μεταβλητών προέρχεται αποκλειστικά από την επιλογή του R. Μπορούμε να θεωρήσουμε την ομοιόμορφα τυχαια συνάρτηση R σαν να διαλέγει μια τυχαία έξοδο για κάθε είσοδο στο πεδίο ορισμού της. Τότε δεδομένης οποιασδήποτε επιλογής της τιμής του R πάνω σε όλα τα σημεία εκτός από το (w, x) έχουμε

$$E[Q_i] = E[Q(w,x)] = E\left[T(x, u', R(w,x)) - \left(\frac{Count(x,u')}{2^m}\right)\right] = 0 \quad (5.11)$$

Επιπλέον από τις ιδιότητες της διάταξης μας οι μεταβλητές $Q_1, ..., Q_{i-1}$ είναι ανεξάρτητες από το $R(w, x)$ και έτσι προκύπτει το ζητούμενο. ■

Από το Λήμμα 16 έχουμε ότι οι περιορισμοί του G που είναι ακυκλικοί δεν έχουν κακή εξάρτηση. Τώρα θα δείξουμε ότι μπορούμε να χωρίσουμε ολόκληρο το σύνολο των κορυφών $V = \{0,1\}^d$ σε δύο υποσύνολα ίδιου μεγέθους V_1, V_2 έτσι ώστε ο περιορισμός του G σε οποιαδήποτε από αυτά τα δύο σύνολα να είναι ακυκλικός.

Λήμμα 17 *Για κάθε κατευθυνόμενο γράφημα $G = (V, E)$ όπου όλες οι κορυφές έχουν μόνο μία εισερχόμενη ακμή και το $|V|$ είναι άρτιο, υπάρχει μία διαμέριση του V σε V_1, V_2 έτσι ώστε $|V_1| = |V_2|$ και θέτοντας G_b να είναι ο περιορισμός του G στο V_b, και τα δύο γραφήματα G_1, G_2 είναι ακυκλικά.*

ΑΠΟΔΕΙΞΗ. Η βασική παρατήρηση είναι ότι κάθε κορυφή $v \in V$ μπορεί να ανήκει σε ένα το πολύ κύκλο. Μπορούμε να σπάσουμε κάθε κύκλο τοποθετώντας τις μισές κορυφές στο V_1 και τις άλλες μισές στο V_2. Μπορούμε να το κάνουμε αυτό για κάθε κύκλο διαδοχικά κρατώντας τα V_1 και V_2 ισορροπημένα. Στο τέλος θα καταλήξουμε με δύο σύνολα ίσου μεγέθους που και τα δύο είναι ακυκλικά. ■

Συνδυάζοντας τα λήμματα 16,17 μπορούμε να χωρίσουμε το $\{Q(w,x)\}$ σε δύο αριθμημένα σύνολα $\{Q_1^1, ..., Q_l^1\}, \{Q_1^2, ..., Q_l^2\}$ όπου $l = 2^{d-1}$ έτσι ώστε για $b \in \{1,2\}, 1 \leq i \leq l, E[Q_i^b|Q_1^b, ..., Q_{i-1}^b] = 0$. Ας ορίσουμε τις τυχαίες μεταβλητές $S_i^b = \sum_{j=1}^{i} Q_j^b$ για κάθε $b \in \{1,2\}, 1 \leq i \leq l$. Τότε (για $b = 1, 2$) η ακολουθία $S_1^b, ..., S_l^b$ είναι martingale. Τώρα από την εξίσωση 5.10 παίρνουμε

$$\Pr[\bar{Q} > \epsilon] = \Pr\left[\frac{(S_l^1 + S_l^2)}{2^{k+d}} > \epsilon\right] \leq \Pr[S_l^1 > \epsilon 2^{k+d-1}] + \Pr[S_l^2 > \epsilon 2^{k+d-1}] \quad (5.12)$$

$$\leq 2e^{-\frac{1}{16}2^{d+k}\epsilon^2} \tag{5.13}$$

το οποίο προκύπτει εφαρμόζοντας την ανισότητα του Azuma και στους δύο όρους του δεξιού μέλους της (5.12) και παρατηρώντας ότι $|S_i^b - S_{i-1}^b| = Q_i^b \leq 2$. Τώρα, χρησιμοποιώντας αυτήν την ανάλυση μπορούμε να αποδείξουμε το θεώρημα.

Μέχρι τώρα έχουμε θεωρήσει ένα σταθερό αντίπαλο A , distinguisher T και πηγή W έτσι ώστε η (5.13) φράσσει την πιθανότητα αυτά να είναι κακά (δηλαδή η 5.9 δεν ισχύει για αυτά) για μια τυχαία συνάρτηση R. Για να γίνει αυτό σαφές θα συμβολίσουμε την τυχαία μεταβλητή $\bar{Q}$ ως $\bar{Q}(W, A, \mathcal{D})$ και θα ορίσουμε το γεγονός $\mathcal{R}$: για μία τυχαία συνάρτηση R υπάρχει μία πηγή W, αντίπαλος A και distinguisher T τ.ω. $\bar{Q}(W, A, T) \geq \epsilon$, δηλ ότι ο R δεν είναι non malleable extractor .

Θα εφαρμόσουμε ενιαίο φράγμα για όλα τα W, A, T. Έστω $N = 2^n, K = 2^k, D = 2^d, M = 2^m$. Τότε υπάρχουν πιθανές $\binom{N}{K}$ flat k-sources , D^D αντίπαλοι και 2^{DL^2} distinguishers . Οπότε

$$\begin{aligned}\Pr[\mathcal{R}] \leq \Pr\left[\bigcup \bar{\mathcal{Q}}(\mathcal{W}, \mathcal{A}, \mathcal{T})\right] &\leq \sum \Pr[\bar{\mathcal{Q}}(\mathcal{W}, \mathcal{A}, \mathcal{T})] \\ &\leq \binom{N}{K} D^D 2^{DM^2} 2e^{-\frac{1}{16}2^{d+k}\epsilon^2} \\ &\leq e^{K(1+\ln(\frac{N}{K}))+D(\ln D + M^2 \ln 2)+\ln 2 - \frac{1}{16}DK\epsilon^2}\end{aligned} \tag{5.14}$$

Τώρα για να είναι το παραπάνω μικρότερο από 1, αρκεί να ισχύουν οι (5.1),(5.2). Άρα αν ισχύουν οι (5.1),(5.2) υπάρχει non malleable extractor, αφού η πιθανότητα μία τυχαία συνάρτηση R να μην είναι non malleable extractor είναι μικρότερη της μονάδας. ■

Σημείωση Για την περίπτωση που η Εύα έχει επιπλέον πληροφορία Z σχετική με το W, ορίζεται ο non malleable average case extractor , και αποδεικνύεται επίσης ότι υπάρχει [DW09].

Ορισμός 34 *Λέμε οτι μία συνάρτηση* $Ext : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *είναι* (n, k, d, m, ϵ) *non malleable average case extractor,αν για κάθε k-source* $(W|Z)$, *και για κάθε συνάρτηση αντιπάλου* $A : \{0,1\}^d \to \{0,1\}^d$, *έχουμε*

$$(Z, X, Ext(W, A(X, Z)), Ext(W, X)) \sim_\epsilon (Z, X, Ext(W, A(X, Z)), U_m)$$

όπου το X *(seed) είναι ομοιόμορφα κατανεμημένο στο* $\{0,1\}^d$ *και* $A(X) \neq X$.

Θεώρημα 35 *Υπάρχει (n, k, d, m, ϵ) non malleable average case extractor,αν*

$$d > \log(n - k + 1) + 2\log(1/\epsilon) + 7$$

$$k > 2m + 2\log(1/\epsilon) + \log(d) + 9$$

5.2.1 Weak non malleable extractors

Η ιδιότητα της non malleability είναι πολύ ισχυρή. Μέχρι τώρα δεν έχει βρεθεί extractor με αυτήν την ιδιότητα. Για αυτό ορίζουμε μία ασθενέστερη έννοια, του weak non malleable extractor, ο οποίος έχει την ιδιότητα αν $R' = Ext(W, X')$ και $R = Ext(W, X)$, το $(R|R')$ έχει αρκετή ελάχιστη εντροπία. Στην περίπτωση του τελείως non malleable η εντροπία του $(R|R')$ θα ήταν περίπου m. Τώρα θέλουμε να έχουμε κάποια μη μηδδενική εντροπία μικρότερη του m.

Ορισμός 36 *Λέμε οτι μία συνάρτηση $Ext : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ είναι (n, k, d, m, ϵ) weak non malleable extractor,αν για κάθε k-source W, και για κάθε συνάρτηση αντιπάλου $A : \{0,1\}^d \to \{0,1\}^d$, έχουμε*

$$H_\infty(Ext(W, X)|X, Ext(W, A(X))) \geq \lambda(m),\ 0 < \lambda(m) < m$$

όπου το X (seed) είναι ομοιόμορφα κατανεμημένο στο $\{0,1\}^d$ και $A(X) \neq X$.

Ίσως είναι ευκολότερο να βρούμε extractor με αυτήν την ιδιότητα.

Παρακάτω θα επιχειρήσουμε επιθέσεις σε γνωστούς extractors, για να δούμε κατά πόσο είναι non malleable ή weak non malleable.

5.3 Επιθέσεις για malleability

Μια επίθεση για malleability σε έναν extractor συνίσταται στο να επιλέξουμε μία πηγή W, και έναν τρόπο για να διαλέγουμε ένα seed X', βλέποντας το πραγματικό seed X, δηλαδή μία συνάρτηση A τ.ω. $A(X) = X', X' \neq X$.

5.3.1 Απλή γενική επίθεση

- Επιλογή του X': δεδομένου του X, διαλέγουμε το X' τυχαία από το $\{0,1\}^d \setminus \{X\}$.
- Επιλογή της πηγής: διαλέγουμε μία οποιαδήποτε flat k-source πάνω στο $\{0,1\}^n$.

Θεώρημα 37 *Για κάθε extractor Ext, και κάθε flat k-source W, εάν* $(X, Ext(W,X)) \sim_\epsilon U_m$ *με* $\epsilon < 2^{m+d}$*, τότε για κάθε* $\delta > 0$ *με πιθανότητα* $(1-\delta)$ *πάνω στην επιλογή του* $x' = A(x)$*, η ελάχιστη εντροπία μετά την απλή επίθεση είναι*

$$H_\infty(Ext(W,X)|X, Ext(W, A(X))) < 2(k-m+l)$$

όπου $\lambda = \log\frac{1}{\delta} + 1$.

ΑΠΟΔΕΙΞΗ. Όπως είχαμε υπολογίσει στο πρώτο κεφάλαιο, αν ε αρκετά μικρό ($\varepsilon < 2^{m+d}$) τότε $H_\infty(Ext(W,X)|X = x') = H_\infty(Ext(W,x')) > m - \log(1/\delta) - 1 = m - \lambda$, ($\lambda = \log(1/\delta) + 1$) για ποσοστό $(1-\delta)$ των x' (δηλ. για τα περισσότερα seeds.)

$$\begin{aligned} H_\infty(Ext(W,x')) > m - \lambda \Rightarrow \\ \max_{R' \in \{0,1\}^m} \Pr[Ext(W,x') = R'] \leq \frac{1}{2^{m-\lambda}} = 2^\lambda \cdot \frac{1}{2^m} \end{aligned} \tag{5.15}$$

Επειδή έχουμε flat k-source , $\forall w \in W \Pr[W = w] = \frac{1}{2^k}$.
Επίσης παρατηρούμε ότι για κάθε R'

$$\begin{aligned} \Pr[Ext(W,x') = R'] = \\ \sum_{w \in W} \Pr[W = w] \cdot \Pr[Ext(w,x') = R'] = \\ \sum_{\{w \in W | Ext(w,x') = R'\}} \Pr[W = w] = \\ \frac{1}{2^m} \cdot |\{w \in W | Ext(w,x') = R'\}| \end{aligned} \tag{5.16}$$

(Δηλαδή η πιθανότητα ο extractor να δώσει R' με seed x', είναι όσο το άθροισμα των πιθανοτήτων των $w \in W$ που αντιστοιχίζονται στο R' με seed x'.)
Θα συμβολίζουμε με $[R']_{x'}$ το $\{w \in W | Ext(w,x') = R'\}$.

$$(5.15), (5.16) \Rightarrow \forall R' \ |[R']_{x'}| \leq 2^{k-m+\lambda}$$

(Δηλαδή το πλήθος των λέξεων w που δίνουν R' με seed x' είναι το πολύ $2^{k-m+\lambda}$.

Για κάθε R, R' αν $|[R']_{x'}| \neq 0$ (αλλιώς οι επόμενες πιθανότητες είναι μηδενικές) ισχύει

$$\Pr[Ext(W,x) = R | Ext(W,x') = R'] = \frac{|[R]_x \cap [R']_{x'}|}{|[R']_{x'}|} \geq \frac{1}{|[R']_{x'}|}$$

$$\Rightarrow \max_R \Pr[Ext(W,x) = R | Ext(W,x') = R'] \geq \frac{1}{|[R']_{x'}|} \geq \frac{1}{2^{m-\lambda}} \tag{5.17}$$

Παίρνουμε μέση τιμή ως προς R'

$$\begin{aligned} E_{R'} \max_R \Pr[Ext(W,x) = R | Ext(W,x') = R'] &\overset{(5.17)}{\geq} \\ E_{\{R' || [R']_{x'} | \neq 0\}} \cdot \frac{1}{2^{m-\lambda}} + 0 &= \\ \sum_{\{R' || [R']_{x'} | \neq 0\}} \Pr[Ext(W,x') = R'] \cdot \frac{1}{2^{m-\lambda}} &= \\ \sum_{\{R' || [R']_{x'} | \neq 0\}} \frac{|[R']_{x'}|}{2^k} \cdot \frac{1}{2^{m-\lambda}} &\geq \\ \frac{2^{m-\lambda}}{2^k} \cdot \frac{1}{2^{m-\lambda}} &= \\ \frac{1}{2^{2(k-m+\lambda)}} & \end{aligned} \tag{5.18}$$

Αυτό γιατί τα R' με $|[R']_{x'}| \geq 1 \neq 0$ (δηλ με μη μηδενική πιθανότητα) είναι τουλάχιστον $2^{m-\lambda}$ στο πλήθος, γιατί αν ήταν $2^{m-\lambda} - 1$ ή λιγότερα , θα είχαμε $\sum_{R'} \Pr[Ext(W,x') = R'] \leq \frac{2^{m-\lambda}-1}{2^{m-\lambda}} < 1$.

Παίρνω τη μέση τιμή ως προς x: Στην παραπάνω ανάλυση δεν παίζει ρόλο το x, άρα

$$E_x E_{R'} \max_R \Pr[Ext(W,x) = R | Ext(W,x') = R'] \geq \frac{1}{2^{2(k-m+\lambda)}}$$

Παίρνω λογαρίθμους και η ελάχιστη εντροπία είναι

$$H_\infty(Ext(W,X) | X, Ext(W, A(X))) < 2(k - m + l)$$

■

Πόρισμα 4 *Με πιθανότητα 1/2 πάνω στην επιλογή του x', η ελάχιστη εντροπία μετά την επίθεση είναι το πολύ $2(k - m + 2) = O(k - m)$.*

Πόρισμα 5 *Αν $k = m$ με πιθανότητα 1/2 πάνω στην επιλογή του x', η ελάχιστη εντροπία μετά την επίθεση είναι το πολύ 4 bits.*

Αυτό το περιμέναμε, γιατί αν $k = m$ τότε έχουμε μία πηγή με 2^m στοιχεία με πιθανότητα 2^{-m} το καθένα, τα οποία διαλέγοντας ένα seed, τα αντιστοιχούμε μέσω του extractor στο $\{0,1\}^m$ ντετερμινιστικά. Για να είναι το αποτέλεσμα

ομοιόμορφο, δηλαδή κάθε στοιχείο του $\{0,1\}^m$ να έχει πιθανότητα 2^{-m}, θα πρέπει η αντιστοιχία να είναι 1-1, που σημαίνει ότι μαθαίνοντας το $Ext(w,x')$ βρίσκεις και το w άρα και το $Ext(w,x)$.

Επίσης να παρατηρήσουμε ότι τα x' για τα οποία ισχύει η παραπάνω ανάλυση (δηλ. τα $(1-\delta)$ σε ποσοστό), είναι τα καλά για τον αντίπαλο, και κακά για τον extractor. Άρα ο extractor αρκεί να αντιστέκεται σε αυτά.

Επομένως αφού για αυτά τα seeds η εντροπία που μένει είναι $O(k-m)$ bits, για να μου μένουν $O(m)$ bits θα πρέπει $m < \frac{2}{3}k$.

Για να μένουν m bits εντροπίας για (κάθε) συγκεκριμένη τιμή του R' που μπορεί να τύχει, πρέπει $m < k/2$ (προκύπτει από την σχέση 5.17).

Αυτό το περιμέναμε και από την πιθανοτική απόδειξη ύπαρξης non malleable extractor, αλλά και επειδή διαισθητικά, μαθαίνοντας τα m bits του ectractor, μαθαίνουμε m bits της αρχικής εντροπίας του W.

5.3.2 Καλύτερη Γενική Επίθεση

Αυτή η επίθεση επιλέγει μία flat k-source για την οποία η εντροπία μετά την επίθεση ελαχιστοποιείται. Θα περιγράψουμε πρώτα την επίθεση, και μετά θα προσπαθήσουμε να την εξηγήσουμε με ένα παράδειγμα.

Περιγραφή: Έστω $[r]_y = \{w \in W | Ext(w,y) = r\}$. Ορίζουμε τις εξής συναρτήσεις.

- $f_1(W, y, y', Ext(W,y), Ext(W,y')) = \Pr[Ext(W,y) = r | Ext(W,y') = r', Y = y] = \frac{|[r']_{y'} \cap [r]_y|}{|[r]_y|}$
- $f_2(W, y, y', Ext(W,y')) = \max_r\{f_1\}$
- $f_3(W, y, y') = E_{r'}[f_2]$
- $f_4(W, y) = \max_{y'}\{f_3\}$
- $f_5(W) = E_y[f_4]$
- $f_6 = \max_W\{f_5\}$

Επομένως έχω την εξής επίθεση.

- Επιλογή της πηγής: Διαλέγω την πηγή W μεταξύ των flat k-sources για την οποία το $f_5(W)$ μεγιστοποιείται.

- Επιλογή του X': Δεδομένων των W και y θα διαλέξω το y' για το οποίο το $f_3(W, y, y')$ μεγιστοποιείται. Δηλ. $A(y) = y'$ τ.ω. $f_3(W, y, y') = \max_z\{f_3(W, y, z)\}$.

Εξήγηση: Υποθέτουμε ότι έχουμε διαλέξει την πηγή, δηλαδή 2^k λέξεις από το $\{0,1\}^n$ με πιθανότητα 2^{-k} η καθεμία.

Κάθε seed y χωρίζει την πηγή σε κλάσεις ισοδυναμίας, ανάλογα με το αποτέλεσμα του extractor για το συγκεκριμένο y. Αν $m < k$ τότε από την αρχή του περιστεριώνα δεν μπορεί να συμβαίνει κάθε κλάση να έχει ακριβώς ένα στοιχείο. (Αν συνέβαινε αυτό τότε μαθαίνοντας το $Ext(w, y')$ για κάποιο y', θα μαθαίναμε και το w άρα και το $Ext(w, y)$).

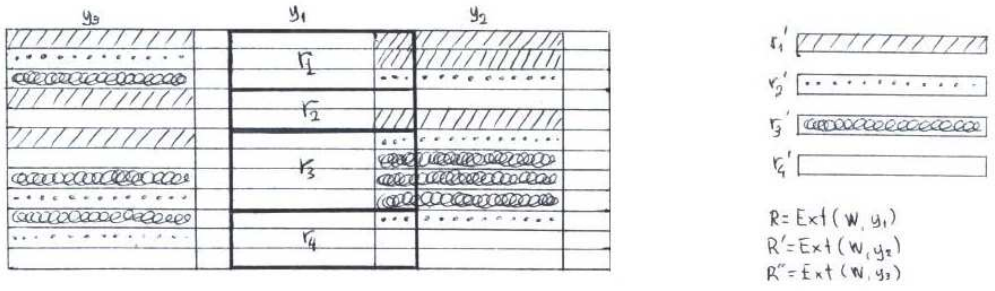
Βλέπουμε το y, δεν βλέπουμε το w και μας ενδιαφέρει να μάθουμε το $R = Ext(w, y)$.

Έχουμε το δικαίωμα να διαλέξουμε ένα y' και να μάθουμε το $R' = Ext(w, y')$ για την ίδια τιμή του W. Το y' χωρίζει την πηγή τις κλάσεις $[R']_{y'}$. Ξέροντας το R', πιθανές λέξεις είναι όσες βρίσκονται στην κλάση $[R']_{y'}$ προφανώς, αλλά το κάθε $r = Ext(w, y)$ έχει διαφορετική πιθανότητα που καθορίζεται από το πόσα από τα $w \in [R']_{y'}$ ανήκουν στην κλάση $[r]_y$. Αυτήν την πιθανότητα εκφράζει η f_1.

Επειδή μας ενδιαφέρει η ελάχιστη εντροπία του R, παίρνουμε την μέγιστη πιθανότητα μεταξύ των τιμών του R, δηλ την f_2.

Επειδή δεν γνωρίζουμε εκ των προτέρων το $R' = Ext(w, y')$ παίρνουμε τη μέση τιμή για όλες τις τιμές του, δηλ την f_3. (Αυτή είναι δεδομένων των y, y' και της πηγής W.)

Επειδή θέλουμε το καλύτερο y', δηλαδή αυτό που θα ελαχιστοποιήσει την μέση εντροπία του R, διαλέγουμε αυτό για το οποίο η f_3 μεγιστοποιείται (δεδομένων των y και W).



Σχήμα 5.1: Παράδειγμα για την επίθεση

Για παράδειγμα στο σχήμα (5.1) οι γραμμές είναι οι λέξεις της πηγής W,

y_1, y_2, y_3 τρία διαφορετικά seeds που χωρίζουν την πηγή σε κλάσεις $[r_i]_{y_1}, [r_i]_{y_2}, [r_i]_{y_3}$, $i = 1, ..., 4$. Εάν $y = y_1$ τότε ποιό από τα y_2, y_3 θα διαλέγαμε στην επίθεση;

Έστω ότι διαλέγαμε το y_3. Ψάχνουμε το R. Εάν $R'' = r'_1$ (που συμβαίνει με πιθ. 1/4) τότε το R είναι r_1 με πιθανότητα 1/3, r_2 με πιθ. 1/3, r_3 με πιθ. 1/3. Ομοίως αν $R'' = r'_2, r'_3, r'_4$. Επειδή δεν ξέρω εξ αρχής το R'' παίρνω το μέσο όρο των μέγιστων πιθανοτήτων για κάθε R''. δηλ.

$$f_3(W, y_1, y_3) = \frac{1}{4} \cdot \frac{1}{3} + \frac{1}{4} \cdot \frac{1}{3} + \frac{1}{4} \cdot \frac{1}{3} + \frac{1}{4} \cdot \frac{1}{3} = \frac{1}{3}$$

Κάνω το ίδιο για το y_2. Εάν $R' = r'_1$ (που συμβαίνει με πιθ. 1/4) τότε το R είναι r_1 με πιθανότητα 2/3 και r_2 με πιθ. 1/3. Μας ενδιαφέρει η ελάχιστη εντροπία, άρα η μέγιστη πιθανότητα που είναι 2/3 και αυτήν θα λάβω υπ΄ όψιν στο f_3. Αν $R' = r'_3$ τότε $R = r_3$ με πιθ. 1, κλπ. άρα

$$f_3(W, y_1, y_2) = \frac{1}{4} \cdot \frac{2}{3} + \frac{1}{4} \cdot \frac{1}{3} + \frac{1}{4} \cdot 1 + \frac{1}{4} \cdot \frac{2}{3} = \frac{2}{3}$$

Άρα θα διαλέξουμε το y_2.

(Τέλειωσε το παράδειγμα). Τώρα όλα αυτά έγιναν για δεδομένο y. Επειδή όμως δεν ξέρω εξ αρχής (δηλ. πριν διαλέξω την πηγή) την τιμή του y, υπολογίζω για κάθε y το $f_4(W, y) = \max_{y'}\{f_3\}$ και παίρνω την μέση τιμή για όλα τα y, δηλ. την f_5.

Τελικά διαλέγω την flat k-source για την οποία το f_5 μεγιστοποιείται.

Για οποιαδήποτε flat k-source W η μέση ελάχιστη εντροπία μετά την επίθεση $(A(y))$ είναι $H_\infty[Ext(W, Y)|Y, Ext(W, A(Y))] = -\log(f_5)$, ενώ για την πηγή που διάλεξα η εντροπία είναι $-\log(f_6)$ και για έναν συγκεκριμένο extractor αυτήν την τιμή θα θέλαμε να φράξουμε για να δούμε κατά πόσο είναι weak non malleable.

Βέβαια πρέπει να πούμε ότι η πηγή που διαλέξαμε είναι η καλύτερη (δηλ. αυτή που ελαχιστοποιεί τη μέση ελάχιστη εντροπία, μεταξύ των flat k-sources, αλλά δεν ξέρουμε αν είναι η καλύτερη μεταξύ όλων των k-sources.

Πρόταση 12 *Δεδομένης μιας flat k-source W, και για αυτή την επίθεση όπου $A(y) = y'$ τ.ω. $f_3(W, y, y') = \max_z\{f_3(W, y, z)\}$, ισχύει*

$$H_\infty[Ext(W, Y)|Y, Ext(W, A(Y))] = -\log f_5(W)$$

ΑΠΟΔΕΙΞΗ. Από τη μία έχουμε

$$H_\infty[Ext(W, Y)|Y, Ext(W, A(Y))] =$$

$$-\log E_y E_{r'} \max_r \Pr[Ext(W,y)=r|Ext(W,A(y))=r', Y=y]$$

Από την άλλη έχουμε

$$-\log(f_5) = -\log E_y \max_{y'} E_{r'} \max_r \Pr[Ext(W,y)=r|Ext(W,y')=r', Y=y]$$

άρα αρκεί

$$\max_{y'} E_{r'} \max_r \Pr[Ext(W,y)=r|Ext(W,y')=r', Y=y] =$$

$$E_{r'} \max_r \Pr[Ext(W,y)=r|Ext(W,A(y))=r', Y=y]$$

αλλά αυτό ισχύει γιατί

$$A(y) = y' \tau.\omega. f_3(W,y,y') = \max_z\{f_3(W,y,z)\} \Leftrightarrow$$

$$f_3(W,y,A(y)) = \max_z\{f_3(W,y,z)\} \Leftrightarrow$$

$$E_{r'} \max_r \Pr[Ext(W,y)=r|Ext(W,A(y))=r', Y=y] =$$

$$\max_z E_{r'} \max_r \Pr[Ext(W,y)=r|Ext(W,z)=r', Y=y]$$

■

Πρόταση 13 *Δεδομένης μιας flat k-source W, για κάθε άλλη συνάρτηση $A(y), A : \{0,1\}^d \to \{0,1\}^d$, ισχύει*

$$H_\infty[Ext(W,Y)|Y, Ext(W,A(Y))] \geq -\log f_5(W)$$

ΑΠΟΔΕΙΞΗ. Για κάθε άλλη επιλογή $A(y)$ έχω

$$f_3(W,y,A(y)) \leq \max_z\{f_3(W,y,z)\} \Leftrightarrow$$

$$-\log E_y f_3(W,y,A(y)) \geq -\log E_y \max_z\{f_3(W,y,z)\} \Leftrightarrow$$

$$H_\infty[Ext(W,Y)|Y, Ext(W,A(Y))] \geq -\log f_5(W)$$

■

Παρατήρηση. Η εντροπία μετά την τυχαία επίθεση είναι άνω φράγμα για την εντροπία μετά από αυτή την επίθεση, όπως προκύπτει από τις προηγούμενες προτάσεις. Άρα το $O(k-m)$ (για την ακρίβεια $2(k-m+2)$) είναι ένα άνω φράγμα.

5.3.3 Εφαρμογή στον $ax + b \mod p$

Είχαμε δει από το Leftover Hash Lemma ότι η συνάρτηση $Ext(x,(a,b)) = (ax+b) \mod p$, όπου p πρώτος της μορφής $2^\lambda - 1$ και $p > 2^n$, είναι extractor.

Διαλέγουμε μια οποιαδήποτε πηγή W. Βλέποντας το seed y ό,τι και να είναι διαλέγουμε $y' = A(y) = (1,0)$, οπότε $R' = Ext(x,y') = x \mod p$. Είναι 1-1 άρα δε μένει καθόλου εντροπία.
(Αν $y = (1,0)$ τότε μπορούμε να διαλέξω π.χ. το $y'' = (1,1)$, και η $x+1 \mod p$ είναι πάλι 1-1).

Τι θα γίνει αν πάρουμε τα m τελευταία bits του output ($m < k/2$);
Δηλ. αν $Ext(x,(a,b)) = (ax+b) \mod p \mod 2^m$;
Θα επιλέξουμε $y' = A(a,b) = (a, b+1)$. Οπότε $H_\infty(R|R', Y) \simeq 0$ γιατί ξέρουμε ότι έχει αλλάξει μόνο το τελευταίο bit του output, λόγω της μορφής του p $(2^\lambda - 1)$.
Για την ακρίβεια αυτό συμβαίνει για όλα τα R' εκτός αν $R' = 0^m$ που τότε παίρνουμε $R = 1^m$ με πιθ. $1 - \frac{1}{2^{\lambda-m}}$ ή $R = 1^{m-1}0$ με πιθ. $\frac{1}{2^{\lambda-m}}$. Εν πάσει περιπτώσει, η εντροπία που μένει είναι $<< 1$ bit.

Τι θα γίνει αν πάρουμε τα m πρώτα bits?
Ισχύει το ίδιο με πριν, μόνο που τώρα κοιτάμε τη θέση του τελευταίου bit του output.Έστω ότι είναι το i-οστό από το τέλος. Για να αλλάξει μόνο το τελευταίο bit του output, θα διαλέξω το $y' = A(a,b) = (a, b + 2^{i-1})$.

Ανοιχτό ερώτημα. Τι θα γίνει αν πάρουμε m τυχαία bits του output που να καθορίζονται από το seed , ή αν πάρουμε m σκόρπια bits, καθορισμένα εξ αρχής;

5.3.4 Εφαρμογή στον extractor του Trevisan

Όπως είδαμε, για να είναι το αποτέλεσμα του extractor του Trevisan κοντά στην ομοιόμορφη κατανομή, πρέπει $m2^\alpha + 3\log m + 2 + 3\log(1/\epsilon) \leq k$. Η επιλογή παραμέτρων που προτείνει ο Trevisan είναι
$k \leq n, 36 \leq m \leq k/2, 0 \leq \epsilon < 2^{-k/2}, \alpha = \log(k/2m)$
και από το σχεδιασμό τα τυχαία bits που χρειάζονται είναι $d = e^{\frac{\ln m}{\alpha}} \cdot \frac{l^2}{\alpha}$.

Αν $m = k/4$ τότε $\alpha = 1$ και $d = ml^2$.
Δηλαδή έχουμε πολλά αχρησιμοποίητα bits στο seed , αφού χρειαζόμαστε το πολύ ml. Αν αλλάξουμε ένα από αυτά, το output δεν αλλάζει καθόλου.

Ανοιχτά ερωτήματα .

Τι γίνεται στον extractor του Trevisan με πιο χρήσιμες επιλογές των παραμέτρων; Δηλαδή όταν $m = k^{1-\gamma}$ με γ σταθ. οπότε $d = O(\log n)$.

Τι γίνεται αν χρησιμοποιήσουμε weak design (όπου $d = \lceil \frac{l}{\ln \rho} \rceil l$) , ή άλλο σχεδιασμό;

Υπάρχει επιλογή παραμέτρων, σχεδιασμού και κώδικα διόρθωσης λαθών έτσι ώστε ο extractor του Trevisan να είναι non malleable ή weak non malleable;

Βιβλιογραφία

[1] B. Chor and O. Goldreich, Unbiased bits from sources of weak randomness and probabilistic communication complexity, SIAM J. Comput. 17(2) (1988), 230-261.

[2] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. Proceedings from Advances in Cryptology - EuroCrypt, 2004.

[3] Yevgeniy Dodis, Daniel Wichs: Non-malleable extractors and symmetric key cryptography from weak secrets. STOC 2009:601-610

[4] O. Goldreich and A. Wigderson, Tiny families of functions with random properties: A quality-size trade-off for hashing, in "Proceedings, 26th Annual ACM Symposium on the Theory of Computing, ACM, 1994," pp. 574-583.

[5] R. Impagliazzo, L. Levin, and M. Luby, Pseudo-random generation from one-way functions, in "Proceedings, 21st Annual ACM Symposium on the Theory of Computing, ACM, 1989," pp. 12-24.

[6] Leighton, FT Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes, Morgan Kaufmann, 1992.

[7] FJ MacWilliams and NJA Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).

[8] N. Nisan and A. Ta-Shma. Extracting randomness: A survey and new constructions. JCSS: Journal of Computer and System Sciences, 58, 1999.

[9] Noam Nisan, Avi Wigderson: Hardness vs Randomness. J. Comput. Syst. Sci. (JCSS) 49(2):149-167 (1994)

[10] N. Nisan and D. Zuckerman, More deterministic simulation in logspace, in "Proceedings, 25st Annual ACM Symposium on the Theory of Computing, ACM, 1993," pp. 235-244.

[11] N. Nisan and D. Zuckerman. Randomness is linear in space. Journal of Computer and System Sciences, 52(1):43-52, February 1996.

[12] Ran Raz, Omer Reingold, and Salil Vadhan. Extracting all the randomness and reducing the error in trevisan"s extractors. jcss, 65(1):97-128, 2002.

[13] J. Radhakrishnan and A. Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. SIAM Journal on Discrete Mathematics, 13(1):2-24, February 2000.

[14] Sipser, Expanders, randomness, or timeversusspace, J.Comput. and System Sci. 36 (1988).

[15] M. Santha and U. Vazirani, Generating quasi-random sequences from slightly random sources, J. Comput. System Sci. 33 (1986), 75-87.

[16] A. Srinivasan and D. Zuckerman, Computing with very weak random sources, in "Proceedings, 35th Annual IEEE Symposium on the Foundations of Computer Science, IEEE, 1994."

[17] Luca Trevisan. Extractors and pseudorandom generators. Journal of the ACM, pages 860-879, 2001.

[18] W. Trappe and LC Washington, Introduction to Cryptography with Coding Theory, Prentice Hall, 2002.

[19] Andrew Chi-Chih Yao: Theory and Applications of Trapdoor Functions (Extended Abstract) FOCS 1982: 80-91

[20] D. Zuckerman, Generalweakrandomsources, in "Proceedings, 31st Annual IEEE Symposium on the Foundation of Computer Science, 1990," pp. 534-543.

[21] D. Zuckerman. Simulating BPP using a general weak random source. Algorithmica, 16(4/5):367-391, October/November 1996.