Κρυπτογραφικά Ασφαλείς Γεννήτριες Ψευδοτυχαίων Αριθμών : Blum Blum Shub Generator

Διονύσης Μανούσακας

31-01-2012

Πού χρειαζόμαστε τυχαίους αριθμούς;

- Σε κρυπτογραφικές εφαρμογές
  - κλειδιά κρυπτογράφησης
  - αρχικοποίηση αλγορίθμων κρυπτογράφησης & υπογραφών
- Σε άλλες αλγοριθμικές εφαρμογές
  - randomized algorithms (tool-box for economical use of randomness)
  - simulation

Ορισμοί

Ορισμός (Γεννήτρια (Γνησίως) Τυχαίων Bits -True Random Bits Generator)

Γεννήτρια Γνησίως Τυχαίων Bits ονομάζεται ένας αλγόριθμος που παράγει ανεξάρτητα και αμερόληπτα bits.

Ορισμός (Γεννήτρια Ψευδοτυχαίων Bits - Pseudo-Random Bits Generator)

Γεννήτρια Ψευδοτυχαίων Bits (PRBG) λέγεται ένας ντετερμινιστικός αλγόριθμος, ο οποίος με είσοδο μια γνησίως τυχαία δυαδική ακολουθία (seed) μήκους n παράγει μια δυαδική ακολουθία $l(n)$ πολυωνυμικού μήκους ως προς την είσοδο που είναι αδύνατο να διακριθεί αποδοτικά από μια τυχαία ακολουθία.

Χαρακτηριστικά μιας PRBG

1. **Efficiency**: Η έξοδος υπολογίζεται σε πολυωνυμικό χρόνο
2. **Stretching**: Η γεννήτρια επεκτείνει πολυωνυμικά την τυχαία είσοδο
3. **Pseudorandomness**: Η έξοδος είναι υπολογιστικά μη-διακρινόμενη από την ομοιόμορφη κατανομή από οποιονδήποτε παρατηρητή

Κρυπτογραφικά ισχυρή PRBG

2 ισοδύναμοι ορισμοί [Yao]:

1. ξεπερνά όλα τα στατιστικά τεστ πολυωνυμικού χρόνου
2. ξεπερνά τον έλεγχο του *επόμενου bit*

Universal Test (Unpredictability):
Έλεγχος Επόμενου bit $\iff$ Έλεγχος Προηγούμενου bit

Ορισμός (Έλεγχος επόμενου ψηφίου - Next-bit test)

Έστω αντίπαλος $\mathcal{A}$ και μαντείο $\mathcal{O}$. Το μαντείο γνωρίζει μια ακολουθία bits s και ο $\mathcal{A}$ επιτρέπεται να ρωτά το μαντείο για το επόμενο ψηφίο όσες φορές θέλει εφόσον υπάρχει τουλάχιστον 1 bit που δεν του έχει αποκαλυφθεί. Στηριζόμενος στη γνώση των πρώτων l bits ο $\mathcal{A}$ πρέπει να μαντέψει το $l+1$-ο bit.
Ορίζουμε ως πλεονέκτημα του $\mathcal{A}$ την ποσότητα

$$adv_{\mathcal{A}} = |\frac{1}{2} - p_{\mathcal{A}}|,$$

όπου $p_{\mathcal{A}}$ η πιθανότητα επιτυχίας του $\mathcal{A}$.

Ορισμός (Κρυπτογραφικά ισχυρή PRBG)

Θα λέμε ότι μια PRBG είναι κρυπτογραφικά ισχυρή αν είναι ανθεκτική στον έλεγχο επόμενου bit. Αυτό σημαίνει ότι για οποιονδήποτε αντίπαλο πολυωνυμικού χρόνου το πλεονέκτημα $adv_{\mathcal{A}}$ είναι αμελητέο.

Στις PRBGs με μη-κρυπτογραφική εφαρμογή αρκούμαστε συνήθως σε ασθενέστερες έννοιας αφάλειας (απλούστερα στατιστικά τεστς)

Αλγόριθμος Blum Blum Shub

1: $p \neq q, p, q \in_R Primes_{Blum}$
$n := pq$
2: $s \in_R \mathbb{Z}_n^*$
$x_0 := s^2 \mod n$
3: **for** i=1,2,... **do**
4: $x_i := x_{i-1}^2 \mod n$
5: $z_i := parity(x_i)$
6: **end for**

Ορισμός (Blum Prime)

Ένας πρώτος αριθμός R καλείται πρώτος κατά Blum (BP) εάν $p \equiv 3 \pmod 4$.

Ορισμός (Τετραγωνικό Υπόλοιπο -QR)

Ένας ακέραιος $x \in \mathbb{Z}_n^*$ λέγεται τετραγωνικό υπόλοιπο mod n αν υπάρχει κάποιο $y \in \mathbb{Z}_n^*$: $y^2 \mod n = x$. Διαφορετικά λέγεται μη-τετραγωνικό υπόλοιπο. Συμβολίζουμε το σύνολο των τετραγωνικών υπολοίπων mod n ως QR_n και το συμπλήρωμά του ως QNR_n.

Ορισμός (Σύμβολο Legendre)

Έστω p περιττός πρώτος. Για $a \in \mathbb{Z}_p$ το σύμβολο Legendre ορίζεται ως εξής:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p|a \\ 1 & a \in QR_p \\ -1 & a \in QNR_p \end{cases}$$

Ορισμός (Σύμβολο Jacobi)

Έστω n περιττός ακέραιος με παραγοντοποίηση $n = \prod_i p_i^{e_i}$ Για $a \in \mathbb{Z}_n$ το σύμβολο Jacobi ορίζεται ως εξής:

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i}$$

Θεώρημα

Έστω $n = pq$ το γινόμενο δύο διακεκριμένων περιττών πρώτων και $\mathbb{Z}_n^*(+1)$ (αντ. $\mathbb{Z}_n^*(-1)$) οι αριθμοί στο $\mathbb{Z}_n^*$ με σύμβολο Jacobi +1 (αντ. -1). Τότε ακριβώς τα μισά από τα στοιχεία του $\mathbb{Z}_n^*$ ανήκουν στο $\mathbb{Z}_n^*(+1)$ και τα υπόλοιπα μισά στο $\mathbb{Z}_n^*(-1)$. Τα μισά από τα στοιχεία του $\mathbb{Z}_n^*(+1)$ και κανένα από τα στοιχεία του $\mathbb{Z}_n^*(-1)$ είναι τετραγωνικά υπόλοιπα - οπότε $QR_n \subset \mathbb{Z}_n^*(+1)$.

$\Rightarrow$ διαμέριση του $\mathbb{Z}_n^*$ σε δύο ισοπληθικά ξένα υποσύνολα $\mathbb{Z}_n^*(+1)$, $\mathbb{Z}_n^*(-1)$, εκ των οποίων στο $\mathbb{Z}_n^*(+1)$ ένα ομοιόμορφα επιλεγμένα στοιχείο x παρουσιάζει $1/2$ πιθανότητα να είναι τετραγωνικό υπόλοιπο.

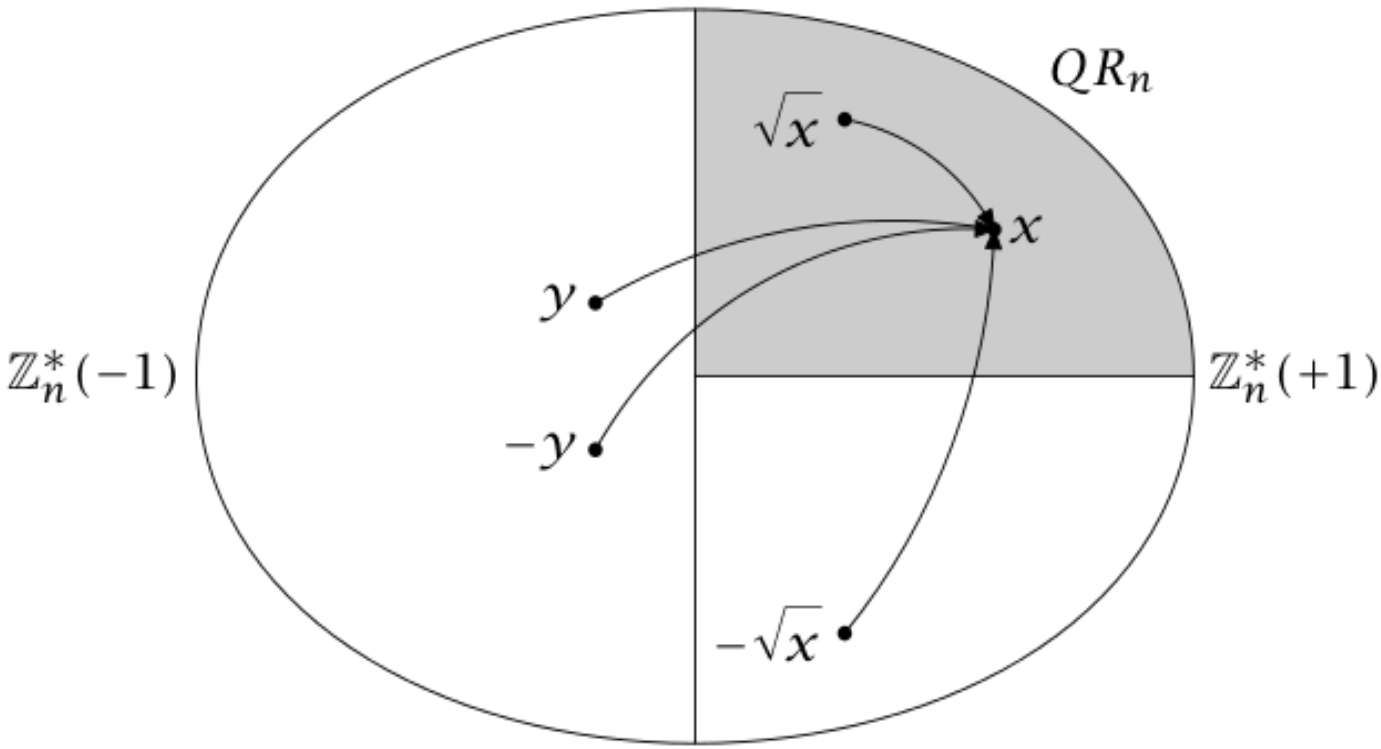
Η ασφάλεια μιας CPRBG έπεται από την υπολογιστική αδυναμία επίλυσης κάποιου αριθμοθεωρητικού προβλήματος που βρίσκεται στον πυρήνα της

Υπόθεση (Υπόθεση Τετραγωνικού Υπολοίπου - QRA)

Κάθε πιθανοτικός αλγόριθμος πολυωνυμικού χρόνου P που αποφασίζει εάν είναι τετραγωνικό υπόλοιπο κάποιο $x \in \mathbb{Z}_n^*(+1)$, με $n = pq$, p, q περιττούς πρώτους, παρουσιάζει πιθανότητα επιτυχίας το πολύ $\frac{1}{2} + \epsilon$, όπου το ϵ είναι αμελητέο ως προς το μήκος του n.

Θεώρημα

Έστω $n = pq$ το γινόμενο δύο διακεκριμένων BP αριθμών. Τότε κάθε τετραγωνικό υπόλοιπο x modulo n έχει τέσσερις διακεκριμένες τετραγωνικές ρίζες. Ακριβώς μία από αυτές είναι επίσης τετραγωνικό υπόλοιπο. Στο εξής θα συμβολίζουμε τη ρίζα αυτήν ως $\sqrt{x}$.



Σχήμα: Η εικόνα του $\mathbb{Z}_n^*$

Η ιδέα της απόδειξης

Υποθέτουμε ότι υπάρχει αλγόριθμος $\mathcal{A}$ ο οποίος, δεδομένης μιας ακολουθίας εξόδου του BBS $z_1, z_2, z_3, \ldots$, αποφασίζει το z_0 με κάποια πιθανότητα, δηλαδή προβλέπει ακολουθίες προς τα αριστερά. Δεδομένου τετραγωνικού υπολοίπου x_0, μπορούμε να παραγάγουμε την ακολουθία $z_1, z_2, z_3, \ldots$ και να τη δώσουμε ως είσοδο στον $\mathcal{A}$. Τότε ο $\mathcal{A}$ θα αποφασίσει την ισοτιμία του z_0 με την ίδια πιθανότητα με προηγουμένως. Ονομάζουμε το νέο αλγόριθμο $\mathcal{A}'$. Θα αποδείξουμε ότι μπορούμε να κατασκευάσουμε ένα νέο αλγόριθμο $\mathcal{B}$ που να αποφαίνεται για την ιδιότητα του τετραγωνικού υπολοίπου με την ίδια πιθανότητα επιτυχίας με την οποία ο $\mathcal{A}'$ αποφασίζει την ισοτιμία, ενώ τρέχει σε πολυωνυμικό χρόνο εάν και ο $\mathcal{A}'$ είναι πολυωνυμικός.

Λήμμα

Αν $n = pq$ το γινόμενο δύο διακεκριμένων περιττών πρώτων, τότε

$$x \in QR_n \iff x \bmod p \in QR_n \wedge x \bmod q \in QR_n$$

Λήμμα

Αν p περιττός πρώτος, τότε

$$p \equiv 3 \pmod 4 \ (Blum) \iff -1 \in QNP_p$$

.

Λήμμα

Έστω $n = pq$ το γινόμενο δύο διακεκριμένων Blum πρώτων. Τότε τα x και $-x$ έχουν το ίδιο σύμβολο Jacobi.

Λήμμα

Η συνάρτηση $x \to x^2$ είναι $2-1$ συνάρτηση στο $\mathbb{Z}_n^*(+1)$, όπου $n = pq$ το γινόμενο δύο διακεκριμένων Blum πρώτων.

Λήμμα

Έστω $n = pq$ το γινόμενο δύο διακεκριμένων Blum πρώτων. Τότε για κάθε $x \in \mathbb{Z}_n^*(+1)$ ισχύει ότι

$$x \in QR_n \iff parity(x) = parity(\sqrt{x^2})$$

.

Θεώρημα (Αναγωγή αλγόριθμου ισοτιμίας σε αλγόριθμο τετραγωνικού υπολοίπου)

Δεδομένου αλγόριθμου $\mathcal{A}$ που υπολογίζει την ισοτιμία του $\sqrt{x}$ μπορούμε να κατασκευάσουμε αλγόριθμο $\mathcal{B}$ που αποφασίζει με την ίδια πιθανότητα επιτυχίας για το εάν ο x είναι τετραγωνικό υπόλοιπο.

Απόδειξη.

Δοθέντος του $\mathcal{A}$ ορίζουμε τον $\mathcal{B}$ ως εξής:

$$\mathcal{B}(n, x) = \mathcal{A}(n, x^2 \mod n) \oplus parity(x) \oplus 1.$$

Δείχνουμε ότι οι πιθανότητες επιτυχίας των αλγορίθμων $\mathcal{A}$ και $\mathcal{B}$ είναι ίσες:

$$Pr[\mathcal{A}(n, x)|\mathcal{G} \to n, x \in_R QR_n, r_A \in \{0,1\}^{t_A}] = Pr[\mathcal{B}(n, x)|\mathcal{G} \to n, x \in_R \mathbb{Z}_n^*(+1), r$$

□

- Μετατροπή Monte-Carlo σε σχεδόν πολυωνυμικούς ντετερμινιστικούς
- Κρυπτογραφία δημόσιου κλειδιού:
  - Ο Bob θέλει να στείλει στην Alice ένα εμπιστευτικό μήνυμα μήκους $m = (m_1, m_2, ..., m_n)$ μέσω δημόσιου καναλιού. Η Alice κατασκευάζει και δημοσιεύει έναν αριθμό (δημόσιο κλειδί) $n_A = p_A q_A$, όπου $p_A, q_A \in BP$ (ιδιωτικά κλειδιά), τέτοιο ώστε $n = poly(|n_A|)$.
  - *Κρυπτογράφηση*: Χρησιμοποιώντας το δημόσιο κλειδί της Alice , ο Bob κατασκευάζει ένα one-time pad με τον ακόλουθο τρόπο: επιλέγει τυχαία κάποιο $x_0 \in \mathbb{Z}^*_{n_A}$ και το εισάγει σε μια γεννήτρια BBS παράγοντας ένα one-time pad $z = (z_1, z_2, ..., z_n)$. Ο Bob στέλνει τα $(m \oplus z, x_{n+1})$.
  - *Αποκρυπτογράφηση*: Η Alice , χρησιμοποιώντας το ιδιωτικό της κλειδί, υπολογίζει τα $x_n, x_{n-1}, ..., x_1$, ανακατασκευάζει το one-time pad και εφαρμόζει XOR .

Βιβλιογραφία

- Lenore Blum, Manuel Blum, and Michael Shub. *A Simple Unpredictable Pseudo-Random Number Generator*. SIAM Journal on Computing, 15(2):364–383, May 1986.
- S. Goldwasser and S. Micali. *Probabilistic encryption and how to play mental poker keeping secret all partial information*. In Proc. 14th ACM Symp. on Theory of Computing, pages 365–377, San Francisco, 1982.ACM.
- Martin Geisler, Mikkel Krøigård, and Andreas Danielsen. *About Random Bits*. December 2004.
- Pascal Junod. *Cryptographic Secure Pseudo-Random Bits Generation: The Blum-Blum-Shub Generator*. August 1999.
- Douglas Stinson. *Cryptography Theory and Practise*, 3rd Edition, Chapman and Hall.
- Umesh V.Vazirani and Vijay V.Vazirani. *Efficient and Secure Pseudorandom Generation*. In Proceedings of Symposium on the Foundations of Computer Scince. 1984
- A. C. Yao. *Theory and application of trapdoor functions*. In Proc. 23rd, IEEE Symp. on Foundations of Comp. Science, pages 80–91, Chicago.