

ÜSİMP ULUSAL PATENT FUARI '23

22-23 Kasım 2023

HIZLI VE HAFİF BİR RASTSAL SAYI ÜRETİCİ

- **Sektör:** Elektronik, Bilişim
- **Fikri Hak Koruma Durumu:** Ulusal Patent başvurusu yapıldı, süreç devam ediyor.
- **Başvuru/Tescil Tarihi:** 2018/05933
- **Koruma İstenen Ülkeler:** Türkiye

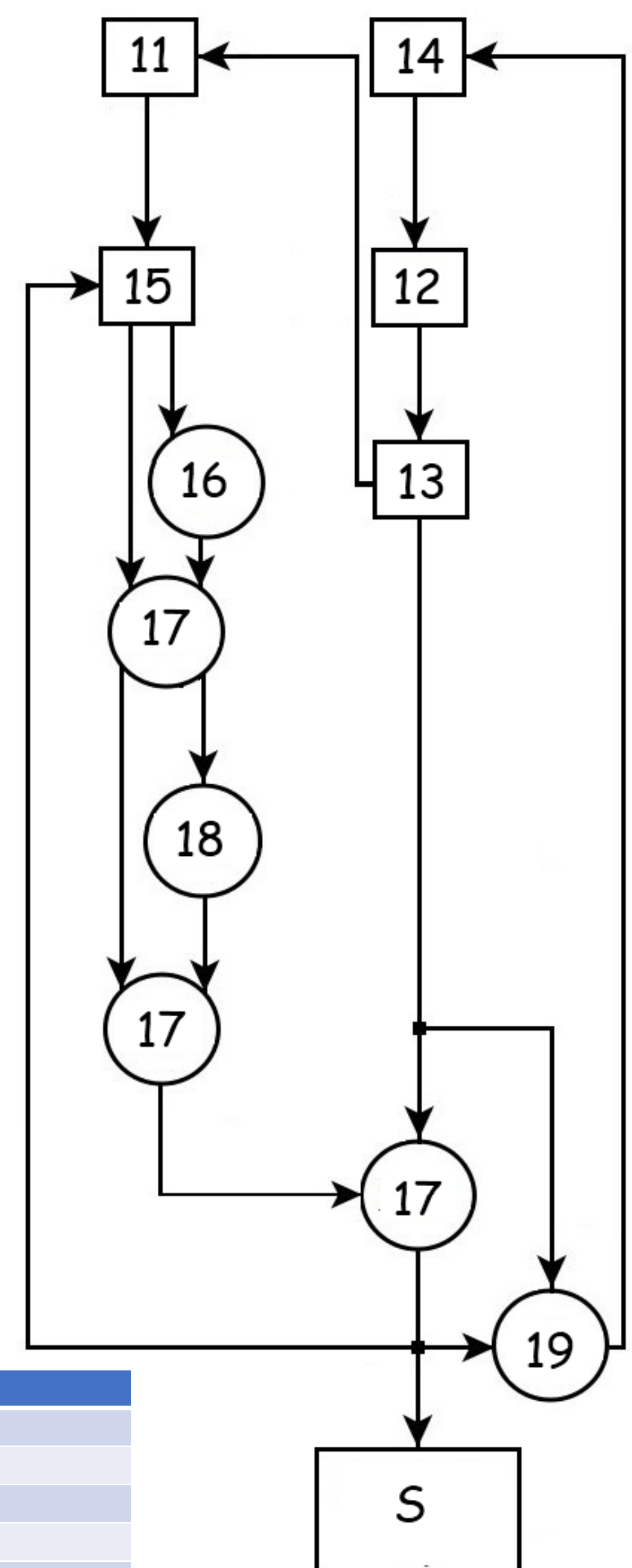
ÖZET

Patente konu olan buluşta “Nesnelerin İnterneti” (IoT) kavramı içinde yer alan düşük kaynaklı cihazlarda kullanılmak üzere bir sözderastsal sayı üretici geliştirilmiştir. Bu yöntem ile günümüzün en büyük sorunlarından olan güvenlik ve mahremiyet konusunda kaynakları kısıtlı cihazlar için önemli bir çözüm üretilmiştir. Bu yöntem, donanım kaynaklarından alınan bir başlangıç değerini alarak seri halinde rasgele sayılar üretmektedir. Bu rastgele sayılar, ilgili cihazların doğrulama ve iletişim güvenliği aşamalarında güvenlik ve mahremiyeti sağlamak için kullanılmaktadır.

TANITIM

Buluş, sözde rastlantısal (rastsal) sayılar üretmeye yarayan algoritmik ve matematiksel yöntem ile bu yöntemi çalıştıran aparattır. Yöntemi meydana getiren adımlar, bunların sırası ve katsayıları tarif edilmiştir. Tüm sayı ve bu sayıların tutulduğu değişkenler, n keyfi bir doğal sayı olmak üzere 2^n bayt boyutunda tanımlanmış olup üretecin çıktı boyutunu, yani üretilen rastsal sayının dijital ortamdaki boyutunu belirlemektedir. Üreteç iki girdi ile başlatılır, tur çalışır ve her turda 1 rastsal sayı üretir. Toplamda, isteğe bağlı olarak (2^n) -1 adete kadar tekrarlanmayan rastsal sayılardan oluşan bir dizi elde edilebilir.

1. 2ⁿ bayt boyutunda ifade edilebilen herhangi iki tamsayı girdi olarak üretece verilir ve tur başlar.
2. İlk girdi sayısı 23 basamak sola ötelenir ve ötelenmeden önceki haliyle XOR işlemine tabi tutulur.
3. Elde edilen sayı 17 basamak sağa ötelenir ve ötelenmeden önceki haliyle XOR işlemine tabi tutulur.
4. Elde edilen sayı üretce bu turda ürettiği bir rastgele sayı çıktısıdır.
5. Bu sayı ile mevcut turdaki ikinci girdinin toplamı bir sonraki turun ikinci girdisi olarak kaydedilir.
6. Mevcut turun ikinci girdisi de bir sonraki turun birinci girdisi olarak kaydedilir.
7. Tur sona erer. İstenirse yeni tura geçilir.



Ref.No.	Ref. Açıklaması
11	İlk sayı girdisi
12	Sayı
13	Sayı
14	İkinci sayı girdisi
15	Sayı
16	Sola öteleme adımı
17	XOR işlem adımı
18	Sağa öteleme adımı
19	Toplama adımı
S	Rastgele üretilen sayı

Beklenti

Ortak Girişim
Ortak Üretim
Yatırım
Lisanslama
Satış

Teknoloji Hazırlık Seviyesi

THS: 6