بسم الله الرحمن الرحیم

گزارش الگوریتم رمز Serpent Plus

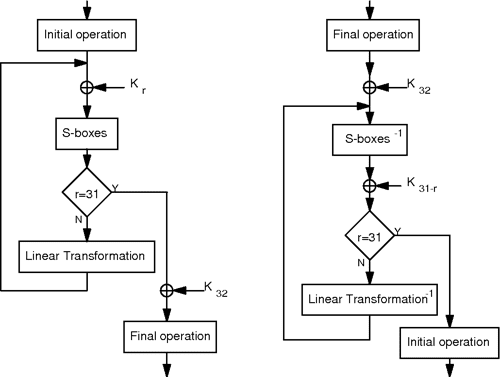
محمد مهدی سوری

عرفان محمدی

**ساختار Serpent**

ابتدا به ساختار الگوریتم Serpent می پردازیم و سپس تفاوت های آن را با Serpent Plus مشخص می کنیم.

الگوریتم Serpent از 32 دور و شبیه شبکه SPN ساخته شده است. ابتدا متن ساده درون Initial Permutation می رود و بیت های آن جا به جا می شود. سپس 31 دور به این صورت انجام می شود که ابتدا با کلید آن دور XOR می شود سپس تبدیل غیر خطی آن در S-Box ها انجام می شود سپس تبدیل خطی بر روی آن اعمال می شود. در دور 31 ام بعد از S-Box با کلید 32 ام XOR شده و عمل Final Permutation بر روی آن اعمال می شود. در شکل زیر این مراحل نشان داده شده است.



**ساختار Serpent Plus**

**Permutation**

برای Initial Permutation و Final Permutation از Permutation الگوریتم DES الهام گرفته شده است. البته با این تفاوت که در DES از 64 بیت تشکیل شده است لذا از جدول 8 8 ساخته می شود اما در اینجا می خواهیم الگوریتم با 160 بیت کار کند لذا از جدول 16 10 تشکیل شده است در نتیجه Final Permutation الگوریتم Serpent Plus مانند الگوریتم DES منظم نیست. در پیوست جدول های Initial Permutation و Final Permutation آورده شده است.

**S-Box**

طبق مقاله Cryptographic Analysis of All 4 4 Bit S-Boxes که توسط Markku-Juhani O. Saarinen نوشته شده است. همه S-Box های ممکن 4 4 بررسی شده است و بهترین های آنها به عنوان Golden مشخص شده است. ما نیز از همین S-Box ها برای طراحی الگوریتم خود استفاده کردیم.

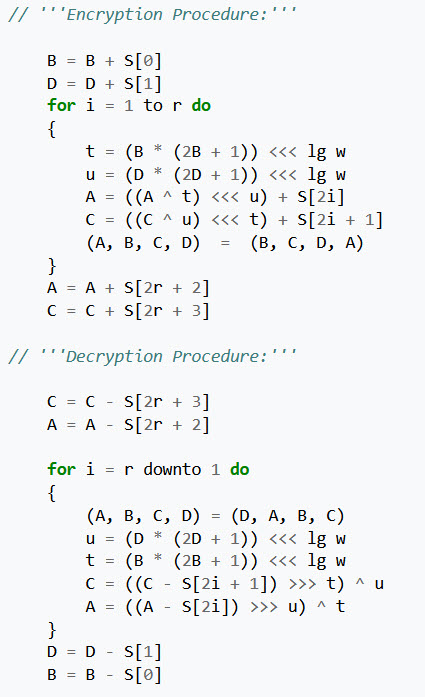
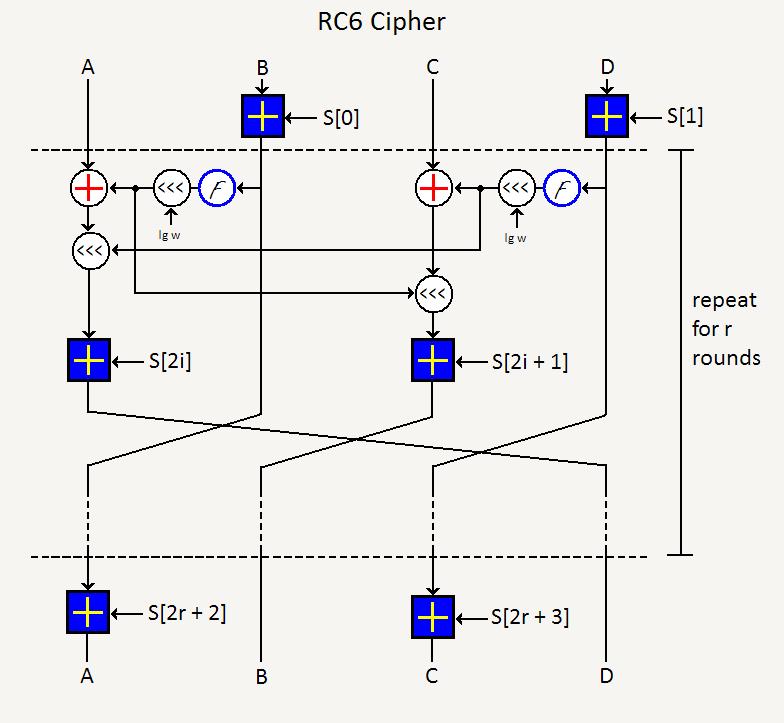
S-Box های مورد استفاده ما همان S-Box های الگوریتم های HummingBird 1 و HummingBird 2 است. چرا که این دو هم جزء Golden ها هستند و هم اینکه ویژگی های تفاضلی و خطی آن نیز مانند S-Box های خود Serpent برابر با است.

S-Box ها در پیوست آورده شده اند.

**Linear Transformation**

در این بخش از یک دور از الگوریم RC6 استفاده کرده ایم. به جای استفاده از کلید از اعداد ثابت مانند رادیکال دو، عدد نپر، عدد پی و نسبت طلایی استفاده کرده ایم که جزئیات آنها را در پیوست آورده ایم.

شکل های زیر نمودار الگوریتم RC6 و کد آن را نشان می دهد.



**Key Scheduling**

از Key Scheduler الگوریم Rijndael استفاده کرده ایم با این تفاوت که ماتریس به صورت است و از S-Box های HummingBird استفاده شده است. بخش R-Con مانند Rijndael است.

**خاصیت Avalanche در الگوریتم Serpent Plus**

ویژگی Avalanche برای حالت کلید ثابت و ورودی های متفاوت اعمال شده است. ابتدا به صورت رندوم 500 ورودی 160 بیتی به حالت Hexadecimal در فایل Input.txt ذخیره شده اند. سپس برای هر دور از الگوریتم ماتریس Avalanche محاسبه شده است نتیجه این است که از دور چهارم به بعد همه اعداد در نزدیکی عدد 250 که حالت مطلوب ما است قرار دارد. اعداد این ماتریس ها به ازای هر دور در فایل هایی در پوشه AvalancheResults قرار گرفته شده است.