6. Conclusion

There is a great improvement in terms of area consumption by using the composite field to implement the S-box compared with the approach using LUTs. In our hardware architecture, we reuse the S-box in F function, which consists of ten 8-bit S-boxes and area occupancy proportion is more than 90%, by dividing each round into 3 clock cycles to reduce the area consumption further. We implemented the proposed design in and synthesized it on 0.18um CMOS technology, the results show that the area is saved by 32.7% by using composite field S-box compared with using LUTs, and 31.2% by reusing S-box compares with not reusing.

7. Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grants 61472208) and National Key Basic Research Program of China (Grant 2013CB338004).

8. References

[1] Leader, G., Paar, C., Poschmann, A., Schramm, K., (2007): New Lightweight DES Variants. In: Biryukov, A. (ed) FSE LNCS, Vol. 4593, pp196-210. Springer, Heidelberg (2007).

[2] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçın, T. (2012): PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer, Heidelberg.

[3] Standaert, F.-X., Piret, G., Gershenfeld, N., Quisquater, J.-J. (2006): SEA: A Scalable Encryption Algorithm for Small Embedded Applications. In: Domingo-Ferrer, J., Posegga, J., Schreckling, D. (eds.) CARDIS 2006. LNCS, vol. 3928, pp. 222–236. Springer, Heidelberg.

[4] De Cannière, C., Dunkelman, O., Knežević, M. (2009) : KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 272–288. Springer, Heidelberg.

[5] Ferhat Karakoc, Hüseyin Demirci. & A. Emre Harmanci, (2013): ITUbee: A Software Oriented Lightweight Block Cipher, Lightsec, LNCS 8162, pp16-27.

[6] Zabotin, I.A., Glazkov, G.P., Isaeva, V.B. (1989): Cryptographic Protection for Information Processing Systems. Cryptographic Transformation Algorithm. Government Standard of the USSR, GOST 28147-89.

[7] D.Canright, , (2005) ,A very compact S-box for AES, Springer.

