～高度情報セキュリティに向けた真性乱数生成用集積回路の研究開発～

委 託 先：㈱東芝
研究代表者：棚本　哲史（藤田　忍）
研究期間：平成14年１月～平成18年３月
主な研究実施場所：神奈川県川崎市

研究成果：情報セキュリティ機能付の超小型LSI内部用に乱数生成回路を開発した。乱数は、パスワード、ID発生といった単純な用途から、暗号鍵の生成や、設計者自身も知りえない初期値の生成、チャレンジレスポンス認証用、機密情報伝送信号の攪拌（耐タンパ）等に使われ、個人情報、電子決済情報、著作権等の機密データを保護する基盤技術である。具体的なターゲットとしては、通常のPC、サーバーや、民生用デジタル機器だけでなく、モバイル機器、さらにはユビキタス社会での携帯機器である。

まず、微細デバイスの新機能として、様々な物理現象を乱数生成デバイスへの展開を検討した（2006年10月3日－10月7日、CEATEC2006）。特に、従来回路との親和性、製造工程としても通常のトランジスタにSiN膜が加わるだけなどの観点から、シリコン窒化膜（SiN）をトラップ層とした乱数源素子（SiN MOSFET）を選び、信頼性、寿命などの研究に注力した。SiN MOSFETの乱数生成メカニズムは、SiN膜と基板との間のトンネル酸化膜が薄いため、多くの電子がSiN膜中のトラップ準位と伝導チャネルの間で往来する確率が大きくなり、ノイズの量が増えるというものである。SiN MOSFET乱数源の高速化（2Mbit／s）に成功した。この改良した乱数生成回路では、通常のCMOSトランジスタに比べて一桁以上の大きなノイズを生成することができる。ノイズが大きいことにより、後段の平滑化回路と増幅率が小さくて済み、回路面積の縮小に繋がった［図１：ISSCC2008（International Solid-State Circuits Conference, 2008年２月　米国／サンフランシスコ）］。そして、ゲート電圧をかける時間を調整することにより10年間安定的に使用できることを確認した（SSDM2010：International conference on Solid State Devices and Materials、2010年９月東京大学）

特許状況　全13件
国内出願　審査中　９件　権利化　５件
外国出願　権利化　２件　審査中　７件

研究成果説明図：

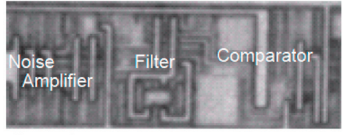

図１　チップ写真