Sujet thèse : Caractérisation, modélisation et quantification du bruit de scintillement et son utilisation comme source d'aléa dans les générateurs de nombres aléatoires

Contexte Scientifique

Les générateurs d'aléa sont des éléments essentiels pour les systèmes cryptographiques. Ils représentent en effet l'unique source de diversité algorithmique, dont la richesse combinatoire (évalué par l'entropie) constitue le seul rempart contre des attaques par force brute (énumération de toutes les possibilités combinatoires).

L'implantation d'un générateur de nombres aléatoires (TRNG – True Random Number Generator) basée sur un processus physique imprévisible dans un circuit intégré ASIC ou FPGA et visant un haut niveau de sécurité est une tâche difficile pour au moins deux raisons : la première est que l'on cherche à implanter un mécanisme volontairement non-déterministe sur une technologie (et avec des outils) dont l'objectif est justement d'assurer le déterminisme de fonctionnement (circuits logiques). La seconde difficulté est que la solution implantée doit impérativement permettre le calcul du taux minimum d'entropie par bit à la sortie du générateur. En effet, l'approche historique consistant à faire passer aux bits générés des tests statistiques génériques [1], [2] pour évaluer la qualité du générateur n'est plus suffisante et ne peut pas conduire à la certification du générateur d'aléa dans les schémas de certification modernes en Europe [3]. Si ces tests restent nécessaires, ils ne sont donc pas suffisants pour prouver l'imprédictibilité du générateur. Il convient alors de proposer une modélisation stochastique de la source d'aléa et du générateur complet afin de pouvoir calculer le taux d'entropie par bit à la sortie du générateur et de prouver ainsi sa sécurité liée à son imprédictibilité.

Peu de solutions techniques répondent à ce jour à la fois aux contraintes d'implantation dans un circuit intégré numérique, et à la capacité de modéliser la source d'aléa et le générateur lui-même pour prouver l'imprédictibilité et l'indépendance des valeurs générées. Ces solutions, souvent à base d'oscillateurs oscillant librement et en particulier les oscillateurs en anneaux (RO - ring oscillators) exploitent en général le bruit électronique intrinsèque à la technologie, et en particulier le bruit d'agitation thermique des électrons. Ce bruit analogique est transformé en instabilité temporelle (la gigue) du signal numérique généré, apparaissant comme un bruit de phase. Ce signal bruité est d'habitude échantillonné par une bascule D afin de produire un bit aléatoire. Un modèle stochastique de la chaine complète est alors mis en place et validé [4] pour estimer l'entropie à la sortie du générateur. Idéalement, ce modèle permet de représenter l'ensemble du TRNG à l'aide de distributions de probabilités qui sont ensuite utilisées pour calculer la probabilité d'apparition d'une séquence de longueur de n bits en sortie du générateur qui peut à son tour être utilisée pour calculer le taux d'entropie par bit du générateur. Ce type de modèle prend en entrée le phénomène physique qui doit être identifié, caractérisé et mesuré précisément afin que le calcul d'entropie grâce au modèle du générateur soit le plus précis possible ou à défaut donne un minorant pour ne pas surestimer le taux d'entropie réel du générateur.

En réalité, deux types de bruits analogiques contribuent au bruit de phase généré par les oscillateurs dans les circuits logiques : le bruit thermique, mais aussi le bruit de scintillement (flicker noise). Aux jours d'aujourd'hui, seul le bruit thermique est pris en compte dans les modèles stochastiques utilisés pour estimer l'entropie, car il est n'est pas auto-corrélé et son modèle est bien connu et validé. Néanmoins, il serait très intéressant d'inclure la contribution du bruit de scintillement au taux d'entropie final à la sortie du générateur. Ceci permettrait d'améliorer la sécurité du générateur tout en réduisant son coût et sa consommation - les critères primordiaux par exemple dans les applications de l'IoT.

Pour terminer cette partie contexte, il est important de mentionner que l'encadrement de cette thèse, que ce soit l'encadrement académique ou l'encadrement industriel, fait partie d'un groupe de travail animé par la DGA-MI sur les problématiques autour de la génération d'aléa. Ce groupe travaille en particulier sur l'élaboration d'un nouveau document de référence donnant un cadre exigeant de certification de générateurs d'aléa visant de haut niveau de sécurité cryptographique. Cette approche de certification est illustrée par des générateurs à base de RO et le taux d'entropie est estimé à partir de la quantification de la gigue causée par le bruit thermique. La caractérisation et la quantification de la gigue provenant du bruit de scintillement et sa contribution au taux d'entropie final pourrait compléter cette approche vers la sécurisation de générateurs d'aléa encore plus poussée.

L'objectif de la thèse sera donc la **caractérisation, la modélisation et la quantification du bruit de scintillement et son utilisation en tant que source d'aléa dans les TRNG basés sur les oscillateurs oscillant librement**, visant des applications cryptographiques d'un haut niveau de sécurité.

Principaux objectifs de la thèse

Le TRNG à base d'oscillateurs oscillant librement et en particulier à base d'oscillateurs en anneaux (RO) et un des types de générateurs le plus largement répandu [5]. Néanmoins, peu de publications scientifiques proposent son modèle stochastique. De plus, les modèles proposés sont basés soit seulement sur la contribution du bruit thermique au taux d'entropie [4], où ils prennent en compte le bruit de phase global, sans différencier la contribution du bruit thermique et le bruit de scintillement [6], ce qui mène à une surestimation d'entropie, très dangereuse pour la sécurité. Plusieurs verrous scientifiques importants restent alors à lever afin de valider les modélisations existantes et/ou de les améliorer.

Le modèle stochastique d'un générateur d'aléa moderne devrait avoir comme paramètre une quantité physique mesurable (de préférence à l'intérieur du circuit). Dans le cas de générateurs utilisant les oscillateurs, cette quantité mesurable peut être la variance de la gigue et en particulier de ce provenant du bruit thermique et de ce provenant de bruit de scintillement. En effet, il est très important de différencier ces deux contributions, car elles n'ont pas la même origine et les mêmes caractéristiques spectrales et temporelles. Un des objectifs de cette thèse sera alors de proposer les méthodes permettant de quantifier et différencier la contribution de ces deux bruits, et qui seront implantables à l'intérieur du circuit.

L'efficacité et la précision de la mesure de contribution de ces deux bruits à la gigue doit être validée par des simulations. Ces simulations peuvent tirer profit du fait que le bruit de scintillement se transforme dans les oscillateurs implantés dans les circuits logiques bruit de phase du signal généré de la même manière comme le bruit thermique. Tandis qu'il est très facile de simuler la contribution du bruit thermique, il ne l'est pas de même pour le bruit de scintillement. En effet, à ce jour, une méthode fiable utilisable pour la modélisation temporaire du bruit de phase provenant du bruit de scintillement n'existe pas.

En conséquence, dans cette thèse nous nous intéresserons aux aspects suivants :

- Etude de l'origine du bruit de scintillement et en particulier de son aspect global et/ou local. Ceci devrait permettre d'étudier le niveau de dépendance entre deux ou plusieurs oscillateurs implantés dans le même circuit et le niveau de dépendance entre les bits à la sortie du générateur. L'étude de ce bruit passera aussi par la réalisation de mes mesures sur composants réels.
- La mise en place d'une modélisation stochastique basée sur le bruit de scintillement, au plus proche du phénomène physique, permettant de modéliser la distribution de probabilité de la phase, et notamment la corrélation entre deux réalisations successives d'échantillonnage de cette phase. Ainsi que la mise en place d'outils de mesure statistique de cette corrélation pour caractériser les paramètres du modèle et le valider ou l'améliorer.
- Proposition d'un modèle temporel du bruit de phase causé par le bruit de scintillement permettant de modéliser les méthodes embarquées de mesure de la gigue et en particulier d'estimer la contribution du bruit de scintillement au bruit de phase global. En outre, ce modèle temporel pourra être utilisé pour générer des séquences de signal bruité pour le développement et la validation en simulation d'architectures de TRNG.
- Validation des modèles stochastiques et temporels en les confrontant aux mesures réelles.
- La mise en place de tests embarqués capables de surveiller, en continu, les paramètres de ces sources de bruit pour vérifier le bon fonctionnement du TRNG

Organisation du travail de thèse

Ce travail de thèse commencera par un état de l'art pluridisciplinaire qui aura pour but de connecter différents domaines scientifiques pour répondre aux problématiques de cette thèse. En particulier :

- Domaine de la sécurité des TRNG : Etude des schémas de certification moderne : AIS31 [3], NIST800-90B [7] et le document de travail du groupe de travail animé par la DGA.
- Domaine de la microélectronique : Etude du bruit de scintillement et de ses origines dans les circuits logiques [8].

- Domaine de la stabilité des horloges : Etude des différentes natures de bruits présents dans les circuits électroniques et leurs impacts sur l'instabilité de la phase d'un oscillateur [9-13].

Suite à cet état de l'art, une connexion forte devra être établie entre la nature des bruits électroniques et leur propagation au sein de l'oscillateur implanté dans un circuit logique pour déterminer la prédominance des bruits qu'on pourra utiliser à la sortie de l'oscillateur pour la génération d'aléa.

Il sera important au cours de l'état de l'art et dans la suite du travail de thèse d'utiliser ou de développer un outil de simulation permettant de simuler l'oscillateur ainsi que les différentes natures de bruits [14] afin de maximiser l'influence de bruits locaux non manipulables dont la contribution à l'entropie du générateur est modélisable. Cette étape de simulation est importante puisqu'en fonctionnement réel, d'autres phénomènes perturbateurs peuvent fausser les mesures. Il conviendra cependant de proposer des mesures internes du bruit de phase provenant du bruit thermique et du bruit de scintillement en sortie de l'oscillateur. Cette étape de simulation sera corroborée par des mesures réelles réalisées sur des composants existants sur lesquels différents paramètres de fabrication technologique varient.

Le résultat de cette étude et des simulations corroborées au mesures réelles, permettra de confirmer ou d'affiner les hypothèses utilisées dans les modélisations existantes.

Dans un deuxième temps, le travail consistera à étudier les dépendances ou corrélations inévitables entre les bits de sortie de l'échantillonneur échantillonnant le signal d'horloge généré par l'oscillateur. Ces dépendances ou corrélations, si elles ne sont pas prises en compte, contribuent à surestimer le taux d'entropie du générateur. Il conviendra donc de les étudier très précisément et encore une fois si possible en simulation d'une part et d'autre part sur des cas d'implantations réelles.

Une fois ces corrélations prises en compte, et les sources de bruit identifiées, il sera possible d'utiliser ou d'affiner les modèles existants afin de calculer le taux d'entropie minimal attendu pour un tel générateur. Des vérifications expérimentales devront alors être faites pour s'assurer que les séquences générées ont une qualité statistique leur permettant de passer des batteries de tests génériques. L'originalité de l'approche consiste à comprendre a priori d'où vient l'aléa et de vérifier a posteriori qu'il n'y a pas de défaut statistique majeur sur les séquences générées ce qui devrait être garanti par le modèle.

Enfin, le travail s'orientera sur la mise en place de tests embarqués dédiés (à l'instar de ce qui est fait dans [15] pour la gigue provenant du bruit thermique dans les RO), basés sur le modèle, afin de détecter toute tentative de manipulation de la source d'entropie. Il est important de noter que ces tests ne sont pas des tests génériques mais des tests visant à estimer précisément les paramètres du modèle afin de garantir qu'ils sont dans un intervalle théorique permettant d'assurer un niveau suffisant d'entropie par bit, ce niveau étant calculé par le modèle.

Niveau de formation exigé

Un diplôme niveau Master est exigé, de préférence dans une des deux orientations suivantes

- Mathématiques/Cryptographie/Informatique/Statistiques
- Physique des semi-conducteurs/Microélectronique

Modalités et encadrement

Cette thèse est proposée dans le cadre d'une collaboration entre le Commissariat à l'Énergie Atomique et aux Énergies Alternatives (CEA-Leti) et le Laboratoire Hubert Curien (équipe SESAM : Systèmes Embarqués Sécurisés et Architectures Matérielles).

Le doctorant sera présent en alternance dans les locaux de CEA-Leti à Grenoble et au sein du Laboratoire Hubert Curien à Saint-Etienne.

Au sein du CEA-Leti le doctorant sera intégré à l'équipe dirigée par M. Mikael CARMONA au Laboratoire de Sécurité des Composants. Il sera encadré scientifiquement par M. Florian PEBAY-PEYROULA.

Au sein du laboratoire Hubert Curien (Université Jean Monnet – CNRS UMR 5516) le doctorant sera intégré à l'équipe SESAM (Systèmes Embarqués Sécurisés et Architectures Matérielles) et encadré scientifiquement par M. Viktor Fischer, Professeur des Universités et par M. Florent Bernard, Maitre de conférences.

Le doctorant sera inscrit à l'Ecole Doctorale ED 488 SIS de l'Université de Lyon sous la direction de M. Viktor Fischer.

Les deux équipes, industrielle et académique, impliquées dans cette thèse disposent des moyens matériels permettant de réaliser des caractérisations et des mesures à l'état de l'art sur des composants intégrés de tous types (microprocesseurs, ASIC, et FPGA). Elles disposent aussi de PC et de serveurs de calculs puissants qui seront mis à la disposition du doctorant.

Références :

[1] Federal Information Processing Standards (FIPS) Publications: FIPS 140--2, Security Requirements for Cryptographic Modules". NIST. May 2001. Retrieved May 18, 2013.

[2] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A Statistical Test Suite for Random and Pseudo-random Number Generators for Cryptographic Applications," tech. rep., National Institute of Standards and Technology, 2010. Special Publication (NIST SP) - 800-22 Rev 1a.

[3] W. Killmann and W. Schindler, “A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators”, standard, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, September 2001.

[4] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux, “On the security of oscillator-based random number generators”. Journal of Cryptology, vol. 24, no. 2, pp. 398–425, 2011.

[5] V. Fischer, P. Haddad, and A. Cherkaoui, "Ring oscillators and self-timed rings in true random number generators". In Y. Nishio (ed.), Oscillator Circuits: Frontiers in Design, Analysis and Applications, IET 2016 (Chapter 13, 26 pages), ISBN: 978-1-78561-057-8.

[6] B. Sunar, W. Martin, and D. Stinson, “A provably secure true random number generator with built-in tolerance to active attacks,” IEEE Transactions on Computers, vol. 56, no. 1, pp. 109–119, 2007.

[7] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, M. Boyle, Recommendation for the Entropy Sources Used for Random Bit Generation, National Institute of Standards and Technology, NIST SP 800-90B, https://doi.org/10.6028/NIST.SP.800-90B

[8] J. A. Barnes, Efficient Numerical and Analog Modeling of Flicker Noise Processes. Forgotten books, Classic reprint series, Aug. 2018.

[9] J. A. Barnes, A. R. Chi, L. S. Cutler, D. J. Healey, D. B. Leeson, T. E. McGunigal, J. A. Mullen, W. L. Smith, R. L. Sydnor, R. F. C. Vessot, and G. M. R. Winkler, “Characterization of frequency stability,” IEEE Transactions on Instrumentation and Measurement, vol. IM-20, pp. 105–120, May 1971.

[10] D. Allan and J. Barnes, “A Modified "Allan Variance" with Increased Oscillator Characterization Ability,” in Thirty Fifth Annual Frequency Control Symposium, pp. 470–475, IEEE, 1981.

[11] W. J. Riley, Handbook of Frequency Stability Analysis, vol. 1065 of NIST special publication. U.S. Department of Commerce, National Institute of Standards and Technology, July 2008.

[12] E. Rubiola, Phase noise and frequency stability in oscillators. The Cambridge RF and microwave engineering series, Cambridge, UK ; New York: Cambridge University Press, 2009. OCLC: 227031868.

[13] N. Da Dalt and A. Sheikholeslami, Understanding Jitter and Phase Noise: A Circuits and Systems Perspective. Cambridge University Press, 1 ed., feb 2018.

[14] N. J. Kasdin and T. Walter, “Discrete simulation of power law noise (for oscillator stability evaluation),” in Proceedings of the 1992 IEEE Frequency Control Symposium, pp. 274–283, IEEE, May 1992.

[15] V. Fischer and D. Lubicz, “Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG,” in Advanced Information Systems Engineering), vol. 7908, pp. 527–543, Berlin, Heidelberg: Springer, Berlin Heidelberg, 2014.