# Un générateur de nombres aléatoires à très faible coût dans une puce RFID

Publié le lundi 24 septembre 2007
Voir en ligne : https://www.france-science.org/Un-generateur-de-nombres.html

Une équipe de trois chercheurs de l'University of Massachussets financée par la NSF vient de publier ses travaux sur la génération de nombre aléatoires dans les puces RFID (Radio Frequency Identification). Ce type de circuit possède par nature des caractéristiques intrinsèques aléatoires qui permettent la génération de tels nombres (délais entre les portes des transistors, gigue électronique, métastabilité). Cependant la lecture de ces valeurs nécessite l'ajout d'un mécanisme de capture annexe à la puce.

Les chercheurs proposent une méthode qu'ils ont baptisée FERNS (pour Fingerprint Extraction and Random Numbers from SRAM - Static Random Access Memory), qui permet d'identifier une empreinte numérique à partir de l'état des transistors de la mémoire de la puce RFID lors de sa mise sous tension. Les cellules SRAM décrites dans l'étude sont composées de six transistors CMOS qui définissent une unité de stockage. Selon le procédé de fabrication, chacune de ces cellules va être initialisée à 0 ou à 1 après la phase de stabilisation qui suit la mise sous tension. Certaines de ces cellules seront invariablement initialisées avec la même valeur, alors qu'un certain nombre d'autres vont osciller entre les deux états à chaque mise sous tension. Des lectures répétées de l'état après initialisation permettent de différencier parmi les unités de mémoire celles qui se stabilisent de façon aléatoire de celles qui prennent toujours la même valeur. Les premières sont alors assimilées à du bruit, alors que les secondes définissent une empreinte numérique caractéristique de chaque puce RFID. Après la caractérisation d'un composant, une simple lecture associée à un filtrage après calcul de la distance de Hamming permet d'identifier de manière unique le circuit.

FERNS permet aussi la génération de nombres aléatoires. Celle-ci découle directement de la distribution elle-même aléatoire des cellules SRAM qui constituent l'empreinte. En effet, la connaissance de la localisation des bits d'identification permet de déduire où sont situés les cellules qui s'initialisent au hasard pour chaque puce. Les 2048 bits de la mémoire (256 octets) sont alors injectés dans une fonction de hachage universelle NH qui permet de générer un nombre aléatoire de 128 bits. Cette clé peut ensuite être utilisée pour crypter les échanges entre la puce et le dispositif de lecture pour la durée de la session (jusqu'à réinitialisation du circuit). Le générateur ainsi réalisé n'est pas lié à un algorithme pseudo-aléatoire (qui au bout d'un moment répète les nombres générés) et a l'avantage d'être intégré par nature au circuit.

Les tests ont été réalisés à la fois sur des étiquettes virtuelles actives, des micro-contrôleurs TI MSP430F 1232 et des puces Intel WISP, chaque composant étant constitué de blocs mémoire de 256 octets. Les résultats montrent que la méthode FERNS appliquée à tous ces dispositifs permet de générer des nombres aléatoires de 128bits qui passent les tests statistiques de cryptographie du NIST (National Institute for Standards and Technology).

Bien que l'extraction d'empreintes numériques à partir de mémoires ait déjà fait l'objet d'études et de brevets (voir "Pour en savoir plus" ci-dessous), la génération de nombres aléatoires constitue une avancée réelle dans le domaine. De plus, le très faible coût de la solution et l'augmentation des mémoires volatiles intégrées aux puces RFID promettent un bel avenir à cette technologie. L'équipe de l'University of Massachusetts va maintenant étudier la vulnérabilité aux attaques de leur solution ainsi que la qualité des empreintes générées.

**Source :**

- NSF researchers produce RFID random number generator, 12/09/2007 - http://www.gcn.com/online/vol1_no1/45018-1.html?topic=authentication&CMP=OTC-RSS
- Ultra-low-cost true randomness AND physical fingerprinting, 10/09/2007 - http://tshb.livejournal.com/2989.html

**Pour en savoir plus, contacts :**

- "Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags", Daniel E. Holcomb, Wayne P. Burleson, et Kevin Fu, 2007 : http://prisms.cs.umass.edu/ kevinfu/papers/holcomb-FERNS-RFIDSec07.pdf
- Slides explicatives associées à la publicaiton "Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags" : http://prisms.cs.umass.edu/ kevinfu/talks/holcomb-FERNS-RFIDSec07-slides.pdf
- "Universal Hash Functions for Emerging Ultra-Low-Power Networks", Kaan Y'uksel, Jens-Peter Kaps, et Berk Sunar, 2004 : http://www.crypto.wpi.edu/Publications/Documents/YukselKapsCnds04.pdf
- Brevet "Method for defining the initial state of static random access memory" : http://www.freepatentsonline.com/6906962.html

Code brève
ADIT : 51117

**Rédacteur :**

Vincent Reboul deputy-stic.mst@ambafrance-us.org