approche DIY
de la sécurité et de l'espionnage électronique

Chauffez ou refroidissez la SRAM

Luka Matic (Croatie)

Nous abordons ici le piratage des données en SRAM (RAM statique) et leur chiffrement par des méthodes non répertoriées qui étendent la capacité de rétention de ces SRAM. Une fois la théorie assimilée, vous pourrez imaginer vos propres variantes ou améliorer et automatiser ce qui est exposé ici. N'hésitez pas à essayer !

Note de l'éditeur : cet article est un extrait du livre intitulé *A Handbook on DIY Electronic Security and Espionage* (« Approche DIY de la sécurité et de l'espionnage électronique ») formaté et légèrement modifié pour correspondre aux normes éditoriales et à la mise en page du magazine *Elektor*. Puisque cet article est extrait d'une publication plus vaste, certains termes peuvent faire référence à des passages du livre d'origine situés ailleurs. L'auteur et l'éditeur ont fait de leur mieux pour l'éviter et seront heureux de répondre aux questions – Pour les contacter, voir l'encadré « Des questions, des commentaires ? ».

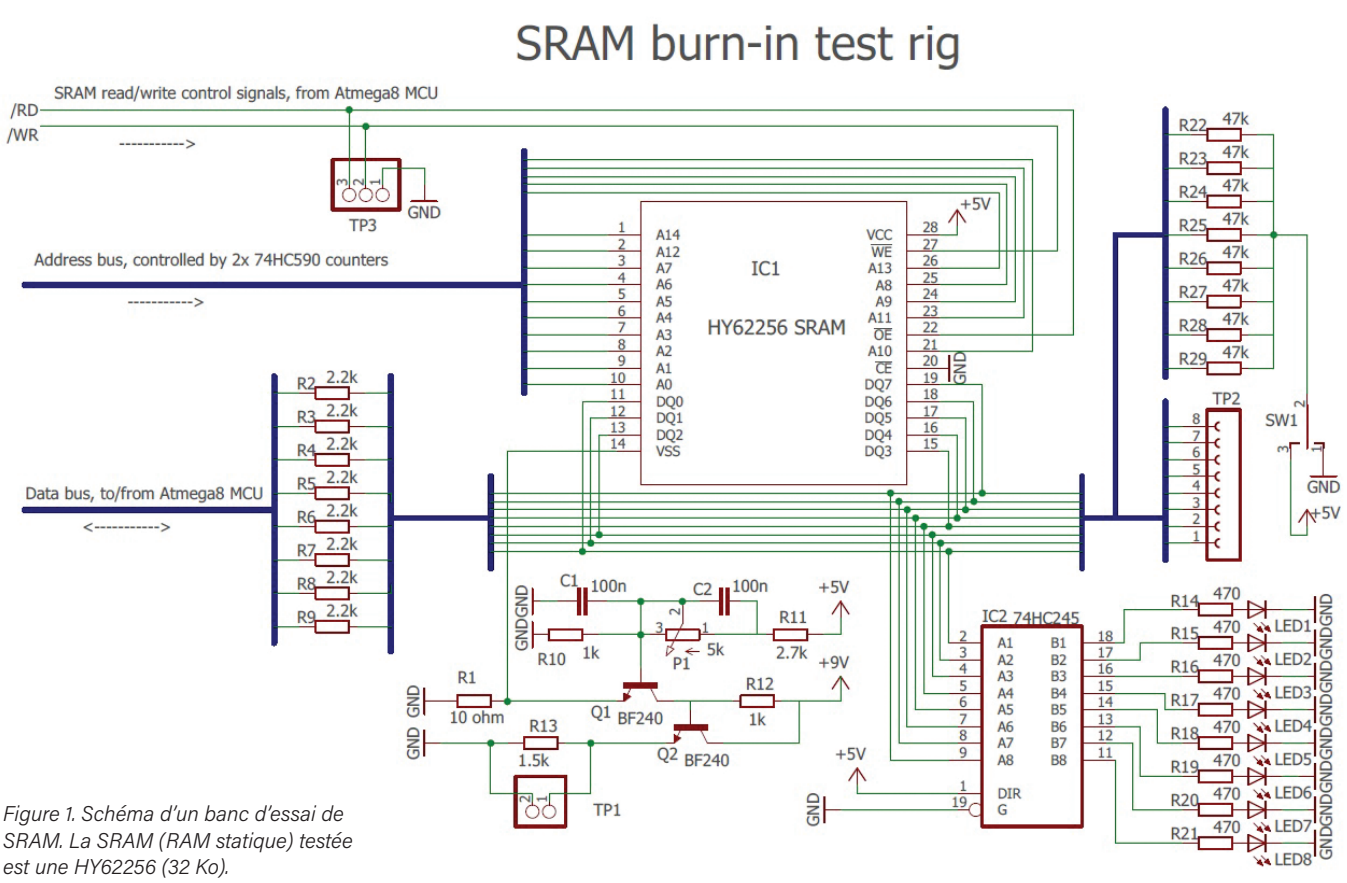


Figure 1. Schéma d'un banc d'essai de SRAM. La SRAM (RAM statique) testée est une HY62256 (32 Ko).

Récupération de données d'après leur empreinte en SRAM

La **figure 1** donne le schéma du banc d'essai utilisé. L'amplificateur analogique à deux étages (Q1 à base commune et Q2 à collecteur commun, pour obtenir la bande passante max.) amplifie la chute de tension sur R1 (image du courant d'alimentation de la SRAM) que l'on observe sur un oscilloscope via le point de test TP1. Un microcontrôleur (MCU) ATmega8 (non représenté sur les schémas) pilote le dispositif. On règle le bus d'adresse sur l'adresse de la mémoire à tester. C'est assez lent, car on utilise deux compteurs à 8 bits 74HC590. C'est acceptable, car il n'est pas nécessaire que l'adresse change vite. Le MCU lit/écrit les données sur le bus et contrôle les commandes /RD et /WR de la SRAM. Ces deux signaux sont utilisés pour déclencher les mesures de l'oscilloscope (point de test TP3). Les résistances R2 à R9 découplent le bus de données, pour le cas où il est activé à la fois par le MCU et la SRAM.

Les résistances R22 à R29 polarisent le bus d'adresses à $+V_{cc}$ ou à la masse (selon SW1) pour mesurer les temps d'accès en lecture et de montée/descente du bus de données, via TP2. Le tampon octal IC2 sert à piloter les huit LED pour faciliter la surveillance du bus de données.

Les variables à mesurer sont le courant consommé en lecture/écriture de la SRAM, et les tensions (c.-à-d. les temps de retard/montée/descente) sur le bus de données. Les variations des signaux mesurés révèlent les marques résiduelles (l'empreinte) des données stockées auparavant et permettent, on l'espère, d'extraire les octets écrits avant que la SRAM ne soit mise hors tension. Pour cela, les cellules SRAM doivent avoir conservé des données figées pour une période relativement longue. Ces durées peuvent varier selon la puce SRAM utilisée.

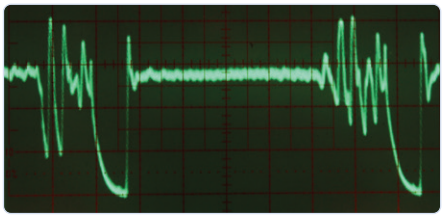


Figure 2. Courant I_{dd} capturé sur un oscilloscope Tek 466 pendant l'écriture des octets 0xDE (à gauche) et 0x01 (à droite) dans la SRAM (à 200 ns/div).

Une résistance de 100 Ω, 5 W plaquée sur la SRAM, avec une sonde de température en sandwich, permet de la chauffer et de la tester à une température élevée, jusqu'à 80-90 °C. Cf. la photo du banc d'essai (fig. 5). Les variations des temps de montée/descente de 1-2 ns doivent être mesurées de manière fiable, ce qui nécessite un oscilloscope à 100 MHz. J'ai utilisé un oscilloscope

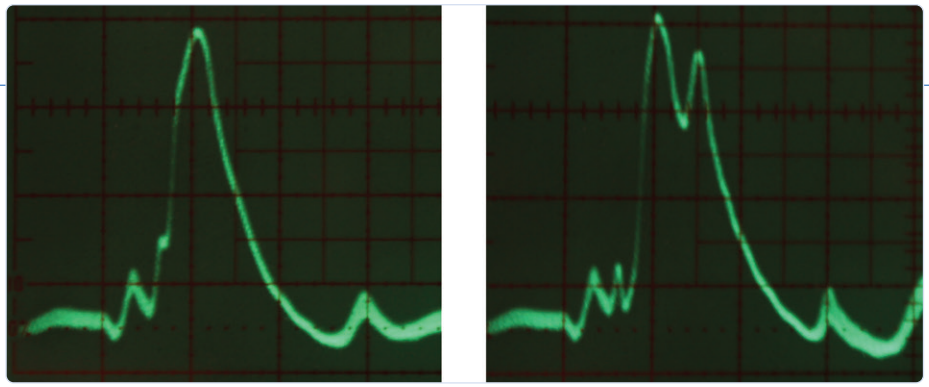


Figure 3. Courant I_{dd} pendant la lecture mémoire de 0xDE (à gauche) et 0x01 (à droite) (à 200 ns/div).

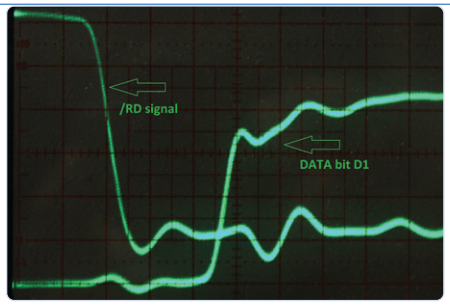


Figure 4. Formes du signal /RD et d'un bit de données lors de la lecture de la SRAM (à 10 ns/div).

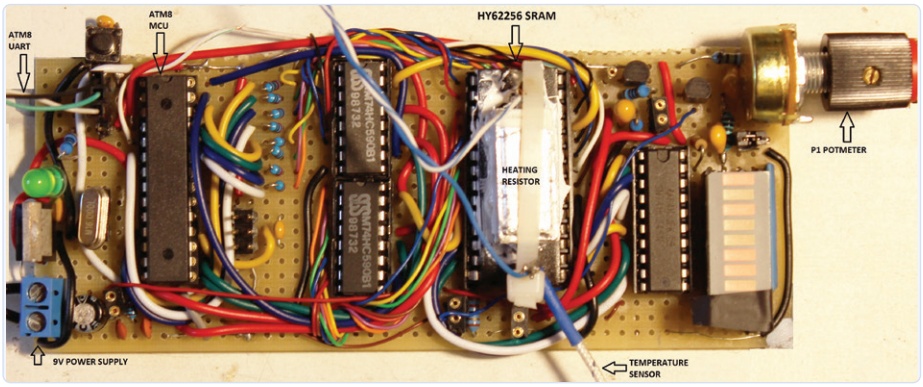


Figure 5. Le banc d'essai de « burn in » des SRAM de l'auteur.

analogique Tektronix 466 vintage à écran à persistance variable avec « flood gun » pour signaux rapides non répétitifs. Sous la rubrique *Rétronique*, *Elektor* a publié un brillant article sur ce type d'oscilloscope à mémoire [1]. La persistance n'est pas indispensable, car les séquences de test de lecture/écriture peuvent être exécutées en boucles répétitives contrôlées par le MCU. J'ai acquis l'oscilloscope Tek 466 à Ljubljana (Slovénie) pour 150 € au marché aux puces électronique.
Commençons par faire à l'oscilloscope quelques mesures de consommation de courant de la RAM et de la tension /RD, cf. **figures 2, 3** et **4**. Les mesures du courant lors de l'écriture et/ou de la lecture de SRAM dans des cellules marquées (ayant longtemps conservé le même octet) ou non (celles dont les bits ont changé sans cesse pendant la même durée), et la comparaison des résultats, peuvent être utilisées pour récupérer les données. La comparaison des temps d'accès en lecture et des formes d'onde (fig. 4) entre les bits sur le bus de données peut également aider à récupérer les données.
La **figure 5** est une photo de mon banc d'expérimentation de la récupération de données en SRAM.

Voici la procédure : j'écris une suite de constantes en SRAM que je laisse ainsi pour la marquer (*burn-in* en anglais). Je programme des compteurs incrémentés toutes les 10 ms dans d'autres cellules SRAM. Je chauffe la SRAM à 80 °C (cela augmente le nombre de porteurs chauds et laisse des traces plus profondes) et je maintiens la puce sous tension pendant 12 h tandis que le MCU continue à incrémenter les compteurs (cela évite de créer des traces dans les cellules concernées). 12 h plus tard, j'éteins la résistance chauffante et la SRAM revient à la température ambiante. Voici le résultat des tests effectués sur deux cellules SRAM :

- à l'adresse 0x204F était stockée une constante (0x66), et on espère qu'elle a pu laisser une trace ;
- à 0x7FF1 tournait un compteur, qui normalement n'a laissé aucune trace.

Les mesures des temps d'accès en lecture (cf. fig. 4) ont montré de très faibles différences (moins d'1 ns) entre les bits « 0 » et « 1 », et je ne les ai donc pas considérées comme pertinentes. Seuls les MOSFET des bistables (qui mémorisent « 0 » ou « 1 ») sont affectés par les effets du *burn-in*. Les MOSFET d'accès à la SRAM et de transfert au bus de données à la lecture ne le sont pas. Cependant, les mesures du courant d'alimentation I_{dd} lors de l'écriture de différents octets dans les cellules marquées ont donné de meilleurs résultats. Cette méthode est meilleure pour d'autres configurations, par ex. pour lire la SRAM depuis un MCU, car elle ne nécessite pas d'accès physique aux 8 bits du bus de données de la SRAM.
Cette fois encore, la cellule à l'adresse 0x204F qui contenait l'octet 0x66 avait subi un *burn-in* à 80 °C. La cellule à 0x7FF1 n'a pas subi de *burn-in* (tous ses bits étant inversés cycliquement). Les mesures (**fig. 6** et **7**) montrent que l'écriture d'un motif octal avec plus de zéros dans une cellule de mémoire marquée consomme plus d'énergie que l'écriture du même motif dans une cellule non marquée. La puissance requise par l'écriture de 0x66 (une valeur marquée) et de 0x99 (complément à 1 de cette valeur) dans une cellule brûlée est notablement plus élevée que dans la cellule non marquée. Mais ces mesures ne suffisent pas à établir l'octet qui a été marqué dans la cellule. Il faut un post-traitement mathématique (filtrage, corrélation avec des motifs connus, etc.).
La SRAM 62256 est un composant ancien assez insensible au marquage par *burn-in*, loin des composants à haute intégration actuels.
Il faut beaucoup d'autres expériences avec d'autres types de SRAM, dans des conditions de marquage variées. Certains auteurs rapportent des résultats contradictoires, ce qui indique donc que les effets résiduels du marquage ne sont ni assez étudiés ni bien compris. Cela ouvre un nouveau et vaste champ de recherche.

Réduction de la tension d'alimentation

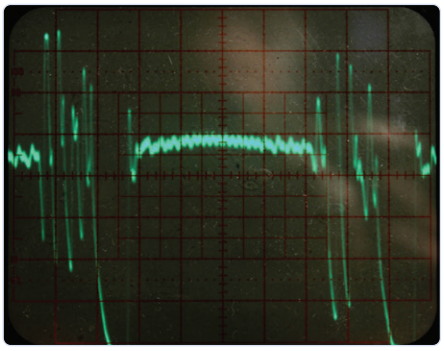
Outre ce que nous avons vu pour extraire les traces de données, il y a une autre approche que je n'ai pas encore essayée. Il s'agit de réduire progressivement la tension d'alimentation jusqu'à ce qu'une cellule de mémoire produise une erreur de lecture ou bien d'écriture. Les cellules marquées et non marquées sont constamment comparées. En général, l'erreur, par ex. lors de l'écriture de 0x00 ou 0xFF, n'affecte que certains bits d'une cellule de mémoire marquée selon l'état de marquage de ces bits (0 ou 1). C'est parce que les tensions de seuil des grilles MOSFET des cellules marquées sont légèrement augmentées ou diminuées par le *burn-in*.

Application

La méthode du « burn-in » pourrait être exploitée pour des communications secrètes améliorées par stéganographie avancée avec de nouveaux types de SRAM à haute intégration plus sensibles au marquage que la « vieille » 62256 testée ici. Une puce SRAM étudiée dans ce but sera utilisable si elle présente un marquage significatif après quelques heures de chauffage à 80 °C (sous tension et avec un message secret chiffré stocké) et si ce marquage persiste pendant 10 à 15 jours une fois la SRAM à température ambiante puis éteinte (retirée du circuit). La méthode de communication fonctionnerait comme suit :

1. L'« expéditeur » Alice chiffre le message secret pour le « récepteur » Bob, et le stocke dans la SRAM.
2. Alice chauffe la SRAM (sous tension et avec le message secret chiffré) à 80 °C pendant 6 à 12 heures.
3. Alice laisse la SRAM refroidir à température ambiante (sous tension).
4. Alice retire du circuit la SRAM refroidie.
5. Alice met la puce SRAM sous enveloppe et l'envoie à Bob.
6. Si l'« espionne » Ève intercepte le courrier, il a simplement l'air de contenir un composant provenant de RS. Même si elle tente de récupérer les données marquées, elle ne verra rien de suspect, car le message est chiffré. Et n'en conclura pas qu'Alice y a caché des données. Peut-être que la puce vient d'être retirée d'un serveur où elle a conservé des constantes pendant très longtemps, par ex. quelques mois à 30 °C.
7. Quelques jours plus tard, Bob reçoit le courrier et exécute la procédure de récupération des données comme ci-dessus.
8. Bob déchiffre le message.

Saurez-vous imaginer d'autres façons dont Alice, Bob, Eve et d'autres pourraient exploiter les effets de persistance de la mémoire SRAM ? Il y en a beaucoup !



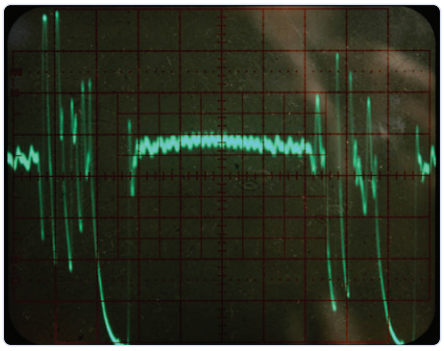
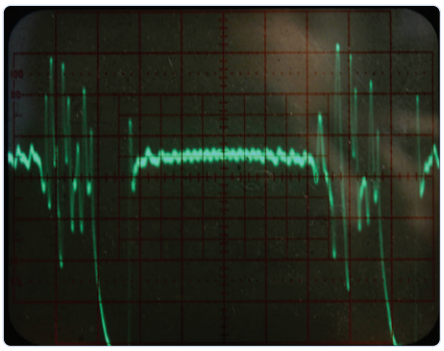


Figure 6. I_{dd} pendant l'écriture des octets 0x00, puis 0xFF à 0x7FF1 (à gauche) et 0x204F (à droite).



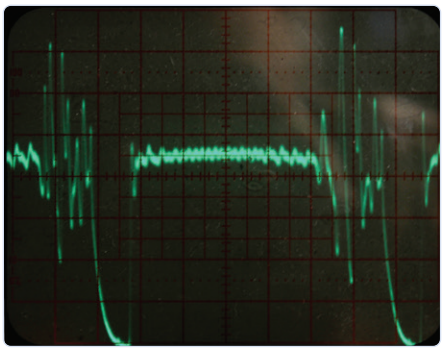


Figure 7. I_{dd} pendant l'écriture des octets 0x66, puis 0x99 à 0x7FF1 (à gauche) et 0x204F (à droite).

Démonstration de l'approche à froid

La 2e démonstration est bien plus simple que la précédente. Le type d'approche à suivre fonctionne probablement pour beaucoup de RAM de types anciens et récents.
Le refroidissement d'une puce jusqu'à –50 °C ne réduit pas de manière significative la conductivité des microcircuits en silicium modérément dopé, et la puce continue de fonctionner normalement, mais hors tension, elle gardera les données, car à –50 °C, les capacités de grille des MOSFET se déchargent très lentement. Le même banc d'expérimentation est utilisé, mais sans résistance chauffante. Des données judicieusement choisies et stockées en SRAM produiront des effets lumineux sur les huit LED du bargraphe. Si ces mêmes effets continuent après la remise sous tension, cela signifie que le contenu de la SRAM est intact. Si des effets irréguliers ou aléatoires apparaissent, c'est que le contenu de la SRAM est perdu. J'ai mesuré le temps maximal de rétention de données à environ –30 °C. C'est facile à atteindre avec un spray réfrigérant (**fig. 8**).
À la température ambiante, les données ne persistent que 0,1 s, mais cela peut atteindre 10 s à –30 °C.
Je refroidis d'abord la SRAM à –30 °C environ et j'augmente progressivement le temps de remise sous tension tout en maintenant la

Figure 8. Spray cryogénique utilisé dans la démo de l'approche à froid.

avec un matériel très bon marché (par ex. l'approche à froid) tandis que d'autres, comme la récupération de traces de données dans la SRAM, peuvent nécessiter un matériel plus sophistiqué et un post-traitement (bien qu'à la portée de l'espion à petit budget !) pour, au-delà de la démonstration du principe, être exploitable en pratique.

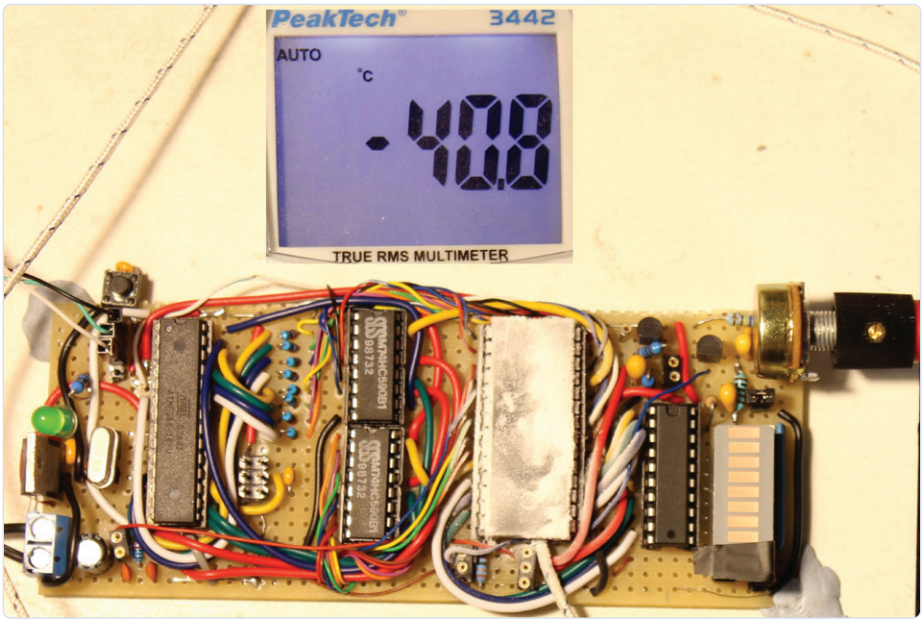


Figure 9. Le circuit intégré SRAM a été refroidi pour obtenir une rétention des données pendant 10 s.

température avec le spray. J'ai atteint un temps de rétention de 10 s à –40 °C (**fig. 9**). Ces résultats étaient attendus, car les broches d'alimentation restent « court-circuitées » par quelques kΩ pendant la mise hors tension, de sorte que la broche V_{dd} peut être considérée comme « à la terre ».

Simplicité surprenante

Comme vu ci-dessus, certaines approches pratiques sont réalisables à la maison

Il ne faut pas oublier que les CI récents à haute intégration sont plus sensibles aux approches présentées. En améliorant les idées évoquées ici, vous pourriez imaginer vos propres dispositifs et procédures d'approche. Il reste beaucoup à faire et donc aucune excuse à l'apathie et à la dépression typiques des ingénieurs du 21e siècle ! Je suis sûr qu'un bon chiffrement à petit budget est possible de nos jours. À mesure que la technologie progresse et que les prix baissent, les choses tournent en faveur d'Alice et de Bob.

210628-04

LIEN

[1] « Tektronix 564 oscilloscope à mémoire (1963) », rubrique Rétronique, Elektor 07-08/2011 : www.elektormagazine.fr/100920

Des questions, des commentaires ?

Envoyez un courriel à l'auteur (luka.matic@gmail.com) ou contactez Elektor (redaction@elektor.fr).

Contributeurs

Texte : **Luka Matic**
Rédaction : **Jan Buiting**
Mise en page : **Giel Dols**
Traduction : **Yves Georges**