CONTRÔLE

Contrôle de connaissances

SR2I301

30 juin 2016

UNE SEULE FEUILLE A4 RECTO/VERSO AUTORISÉE. TOUT AUTRE DOCUMENT, DISPOSITIF DE CALCUL OU DE COMMUNICATION INTERDIT.

3 HEURES

Bon courage !

Questions ouvertes

- ***Pensez à lire les questions en entier (et essayez d'y répondre en entier...)***
- ***Merci d'écrire lisiblement, ce qui ne pourra pas être lu ne sera pas corrigé !***
- *Cet énoncé comporte 5 pages (en plus de la page de couverture).*

Cours d'introduction

Question 1.
Expliquez en quoi un système embarqué est différent, du point de vue de la sécurité, d'un système informatique classique.

Implémentation des algorithmes de cryptographie

Question 2.
Indiquez les principales contraintes auxquelles font face les circuits de cryptographie légère.

Support matériel pour la sécurité logicielle

Question 3.
1. Décrivez brièvement le fonctionnement de la MMU (*Memory Management Unit*) d'un processeur classique.

2. Expliquez comment le système d'exploitation s'en sert pour isoler les processus entre-eux.

3. Indiquez quel autre mécanisme de sécurité offert par les processeurs est nécessaire en complément pour atteindre cet objectif d'isolation.

Analyse par Canaux Auxiliaires (SCA)

TABLE 1 – Bit permutation layer. Chaque bit d'entrée avec index i est déplacé vers position $P(i)$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	4	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

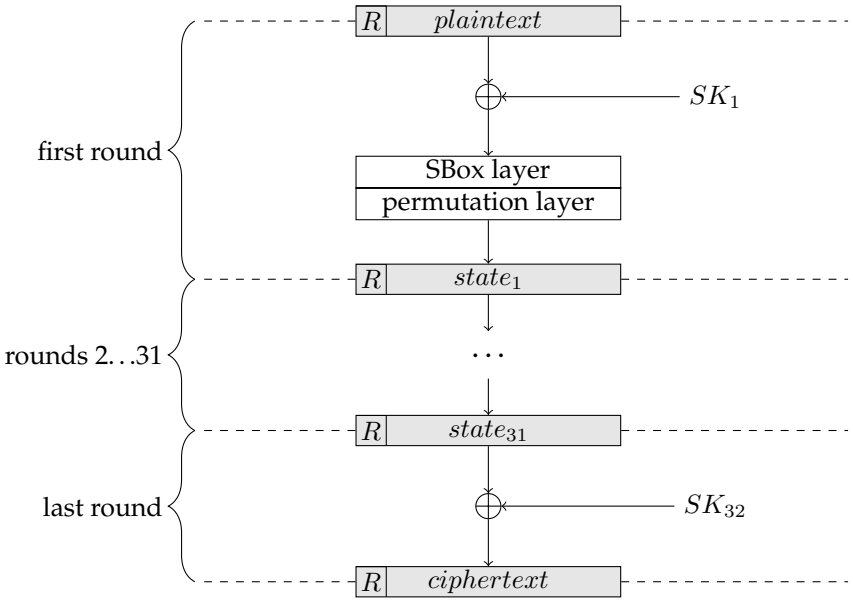

FIGURE 1 – Algorithme global de PRESENT

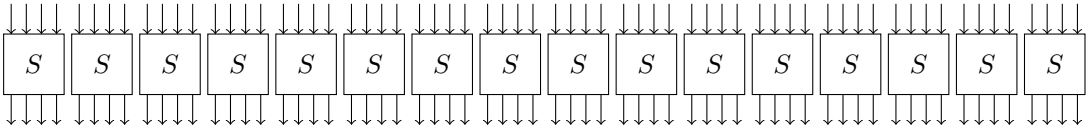

FIGURE 2 – SBox layer avec 16 boîtes S de 4 bits identiques

Question 4.
PRESENT est un algorithme de chiffrement de basse consommation qui chiffre un bloc de 64 bits avec une clé K de 80 ou 128 bits. L'algorithme global est donné dans la figure 1, et il consiste en 31 tours de chiffrement suivi d'un dernier tour plus simple. Dans chaque tour $i \in \{1, \ldots, 31\}$:

1. on calcule le ou exclusif (XOR) du résultat intermédiaire avec une sous-clé SK_i,
2. on passe le résultat par une couche de boîtes S (voir figure 2),
3. on mélange finalement les bits par une couche de permutation (voir table 1).

Dans le dernier tour, on n'applique que le XOR avec la sous-clé SK_{32}. L'unique boîte S réalise une fonction bijective sur quatre bits. Les 32 sous-clés SK_i de longueur 64 bits sont générées à partir de la clé K.

Nous disposons d'une implémentation matérielle itérative de PRESENT. Au début, le registre d'état R de l'implémentation est chargé avec le message en clair P et il est écrit à la fin de chaque tour (voir boîtes grises R dans la figure 1). On suppose que le message en clair P est connu et on va donc attaquer le premier tour.

On voudrait concevoir une attaque en canal caché basée sur la consommation de ce circuit. Donnez un modèle de consommation sur quatre bits qui dépend d'une hypothèse sur les quatre premiers bits $SK_1[0, 1, 2, 3]$ de la sous-clé SK_1. Expliquez votre construction en se basant sur les schémas de l'algorithme.

Question 5.
Détaillez le principe d'une attaque par canaux auxiliaires (SCA) en mesure de consommation (comme par exemple DPA ou CPA) et comment la réaliser. Vous pouvez utiliser les résultat de la question précédente ou vous baser sur un exemple du cours comme le DES. Expliquez le rôle du modèle de consommation et du distingueur.

Question 6.
Pour protéger l'implémentation d'un algorithme de cryptographie, il existe plusieurs contre-mesures. On voudrait évaluer deux protections alternatives :

1. le masquage,
2. un générateur de bruit, réalisé par exemple par un générateur de nombres pseudo-aléatoires.

Expliquez brièvement le principe de ces deux protections et donnez les avantages et les inconvénients de ces solutions.

Attaques par injection de fautes

Question 7.
Donnez deux moyens d'injecter des fautes dans un circuit intégré. Pour chacun, précisez un avantage et un inconvénient.

Question 8.
Donnez deux stratégies de protection face aux attaques par injection de fautes, et pour chacune, deux exemples de mise en œuvre.

TABLE 2 – Table des valeurs $\Delta \mathrm{S}_1(x) = \mathrm{S}_1(\texttt{0x12} \oplus x) \oplus \mathrm{S}_1(\texttt{0x1a} \oplus x)$.

$\Delta \mathrm{S}_1(x)$	x	$\Delta \mathrm{S}_1(x)$	x
0x0	–	0x8	–
0x1	–	0x9	0x14, 0x1c, 0x32, 0x37 0x3a, 0x3f
0x2	–	0xa	0x17, 0x1f
0x3	0x00, 0x01, 0x03, 0x05 0x08, 0x09, 0x0b, 0x0d 0x25, 0x2d, 0x34, 0x3c	0xb	0x04, 0x0c, 0x10, 0x18 0x21, 0x29, 0x33, 0x3b
0x4	–	0xc	0x12, 0x1a, 0x22, 0x26 0x2a, 0x2e, 0x36, 0x3e
0x5	0x15, 0x1d, 0x27, 0x2f 0x31, 0x35, 0x39, 0x3d	0xd	0x11, 0x19
0x6	0x02, 0x06, 0x0a, 0x0e 0x16, 0x1e, 0x20, 0x28	0xe	0x13, 0x1b
0x7	0x24, 0x2c, 0x30, 0x38	0xf	0x07, 0x0f, 0x23, 0x2b

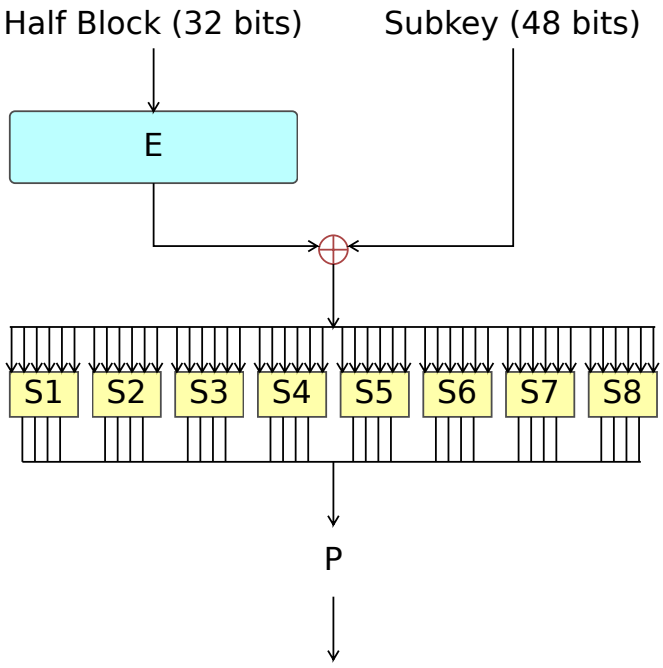

FIGURE 3 – Schéma du calcul de $\mathrm{F}_{K_r}(R_{r-1})$.

Question 9.
On rappelle qu'un tour de DES correspond à calculer :

$$\begin{cases} R_r &= L_{r-1} \oplus \mathrm{F}_{K_r}(R_{r-1}) \\ L_r &= R_{r-1} \end{cases}$$

avec le numéro de la ronde $r \in \{1, \ldots, 16\}$. Par ailleurs, le schéma du calcul de $\mathrm{F}_{K_r}(R_{r-1})$ est représenté sur la figure 3.

1. Exprimez l'équation différentielle générale en sortie d'une boîte S_i en fonction de L_{16} et L_{16}, R'_{16} et R'_{16}, L_{15} et L'_{15}.

2. En déduire et donnez l'équation différentielle réduite dans le cas particulier où la faute ne touche que R_{15}.

3. Dans le cas particulier où $\mathrm{P}^{-1}(R_{16} \oplus R'_{16}) = \texttt{0x00000b00}$, donnez l'index $i \in \{1, \ldots, 8\}$ de la boîte S mise en faute.

4. On suppose maintenant que :
- $K_{16,1} \in \{\texttt{0x07}, \texttt{0x0b}, \texttt{0x14}, \texttt{0x18}, \texttt{0x20}, \texttt{0x2c}\}$
- $\mathrm{E}_1(L_{16}) = \texttt{0x12}$
- $\mathrm{E}_1(L'_{16}) = \texttt{0x1a}$
- $\mathrm{P}_1^{-1}(R_{16} \oplus R'_{16}) = \texttt{0x7}$

À l'aide des réponses précédentes et de la table 2, donnez les valeurs possibles pour $K_{16,1}$.

TRNG & PUFs

Question 10.
Indiquez comment augmenter l'entropie par bit d'un TRNG (*True Random Number Generator*).

Question 11.
Expliquez le principe d'un PUF (*Physical Unclonable Function*) utilisant une mémoire.

Espionnage des bus de communication

Question 12.
Indiquez quel bus (au sens matériel) important, sur la carte mère d'un système embarqué, ne peut pas être protégé (confidentialité et intégrité) en utilisant uniquement une solution logicielle et expliquez pourquoi.

Question 13.
1. Expliquez ce qu'est une attaque par rejeu sur les données transitant sur le bus mémoire d'un système embarqué.

2. Expliquez pourquoi le calcul d'un MAC sur chaque bloc de données à protéger n'est pas suffisant pour contrer ces attaques.

3. Décrivez une solution permettant de s'en prémunir (toujours dans le cadre de la protection du bus mémoire dans un système embarqué).

Contre-façon

Question 14.
Expliquez le principe du *split manufacturing*. Indiquez quels sont ses avantages.
