CRYPTOEXPERTS

WE INNOVATE TO SECURE YOUR BUSINESS

La Cryptographie en boîte blanche: du concept à l'opérationnel

Pascal Paillier

CryptoExperts

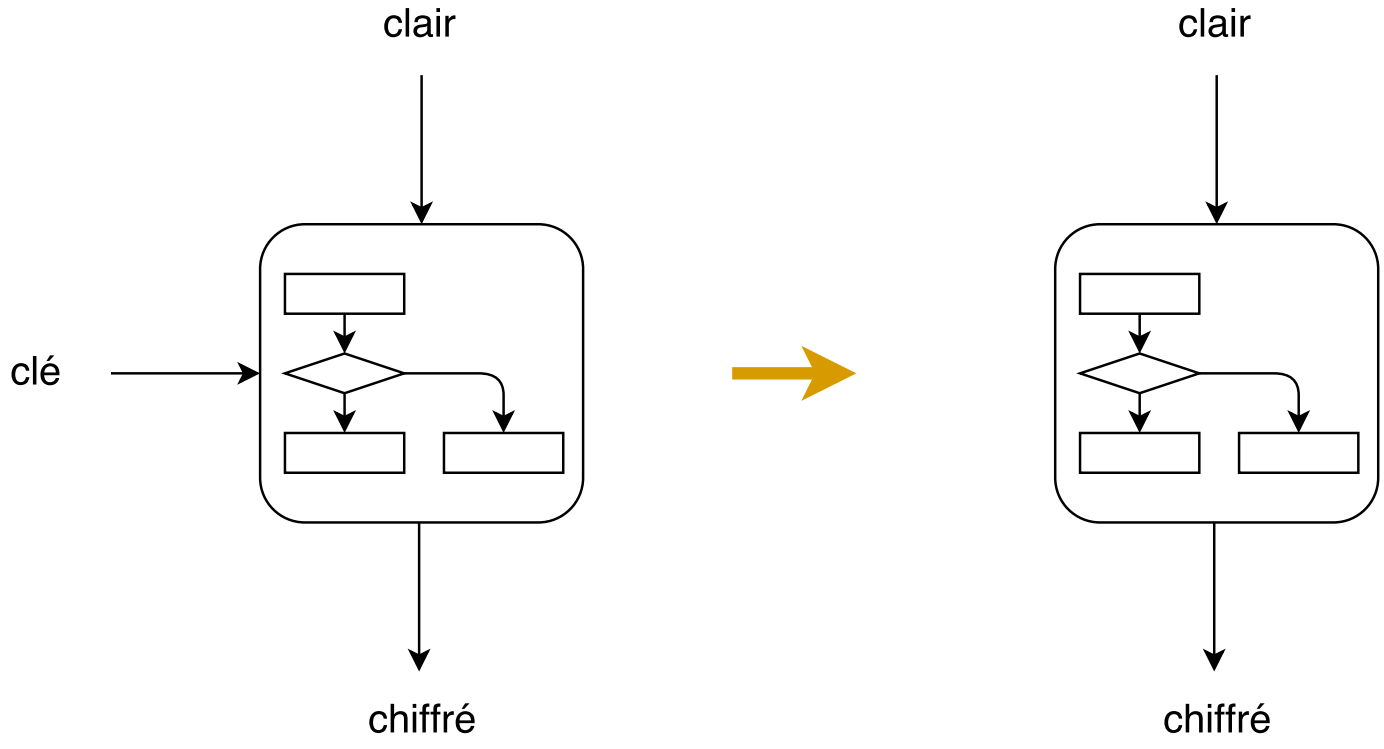
OSSIR – 13 Juin 2017

Aperçu

CryptoExperts

Qu'est-ce que la "white-box crypto" ?

Le concept



L'obfuscation de programmes

Obfuscation de code

- d'un programme P, générer un programme obfusqué $O(P)$
- cacher **toute** propriété π dans le code de $O(P)$
- le code de $O(P) \equiv$ un oracle qui exécute P

L'obfuscation est-elle réaliste?

- **très** fortes exigences sur le compilateur O
- des résultats connus d'impossibilité [BGI+01]
- mais des outils heuristiques existent

Qu'est-ce que la "white-box crypto" ?

$\neq$ obfuscation de programmes!

White-box cryptography [CEJO+02]

- considère des programmes **cryptographiques**

$$\texttt{programs}(f) \quad \text{où} \quad f = \text{fonction sous clé}$$

- cache **certaines** propriétés π du code (mais pas toutes)
- code $\equiv$ un oracle **pour un attaquant contraint**
- déjà des constructions prouvés sûres pour certaines f (f = re-chiffrement [HRSV07,CCV12])
- pas d'impossibilité connue pour f = blockcipher
- mais pas de construction **prouvée** pour e.g. $f = AES_k(\cdot)$

Aperçu

CryptoExperts

Compilateurs en boîte blanche

On choisit $\mathcal{E} = (K, E, D)$ un schéma de chiffrement symmétrique.

Concept

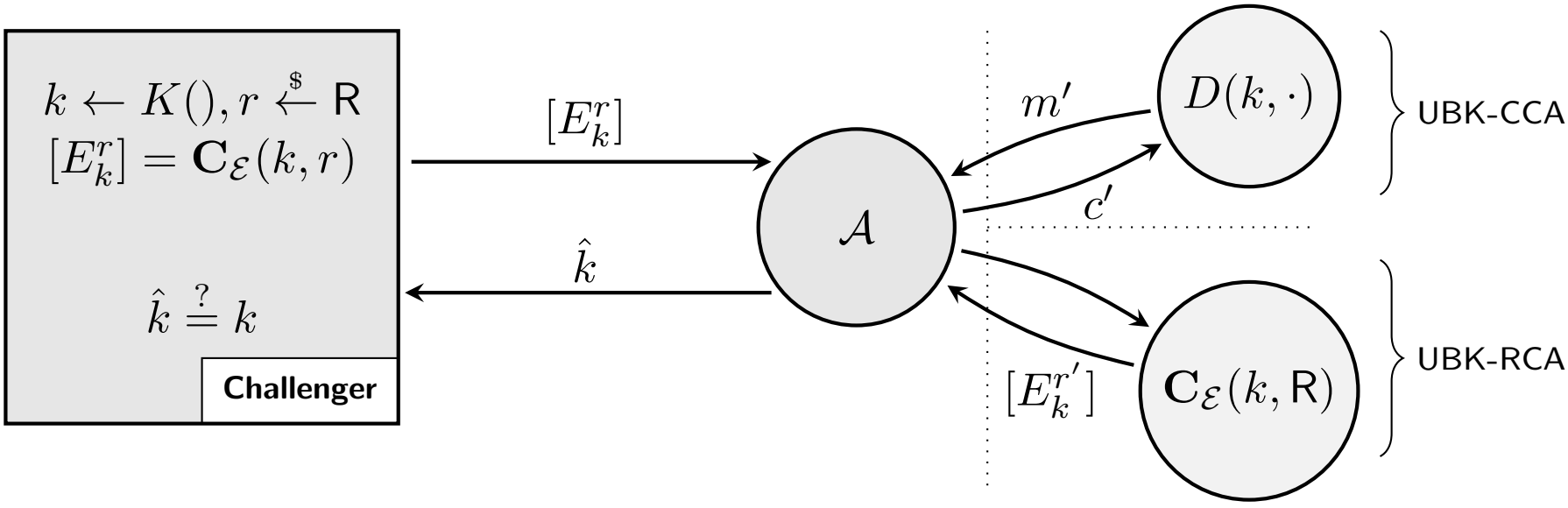
Un compilateur en boîte blanche $\mathbf{C}_{\mathcal{E}}$ prend en entrée une clé $k \in \mathrm{K}$ et un aléa $r \in \mathrm{R}$ et génère un programme $P = \mathbf{C}_{\mathcal{E}}(k, r) = [E_k^r]$.

Ces concepts diffèrent très largement:

fonction $E(\cdot, \cdot)$	**oracle** $E(k, \cdot)$	**programme** $[E_k^r]$
description analytique ou algorithmique	accès externe par entrées/sorties, peut être "stateful"	mot dans un language, "stateless" car relançable, copiable, transférable, observable, modifiable, appel systèmes simulables
(spécification)	(carte à puce/HSM)	(programme exécutable)

CryptoExperts

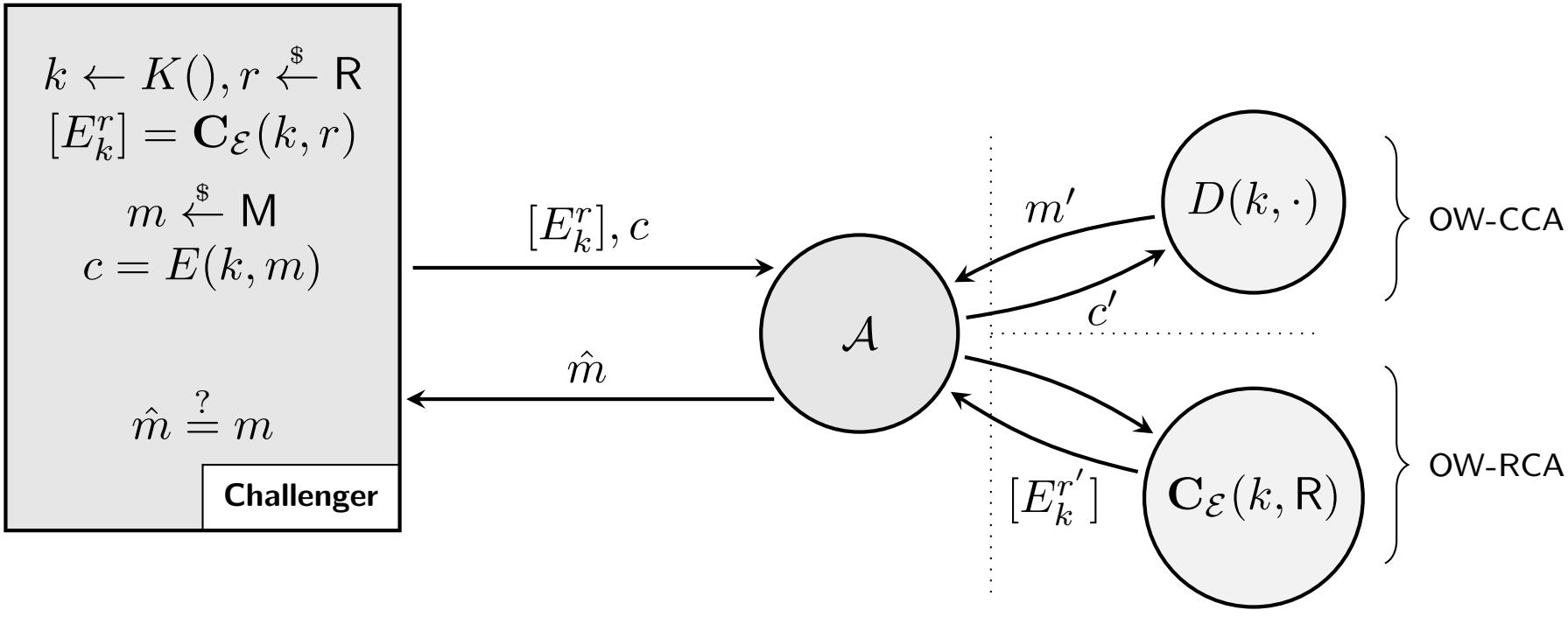
Incassabilité de base (UBK)



Pas de "sécurité sémantique" de la clé k puisque tester si $\hat{k} = k$ est trivial.

Donc une certaine information sur la clé k doit fuir...

Non inversibilité (OW)

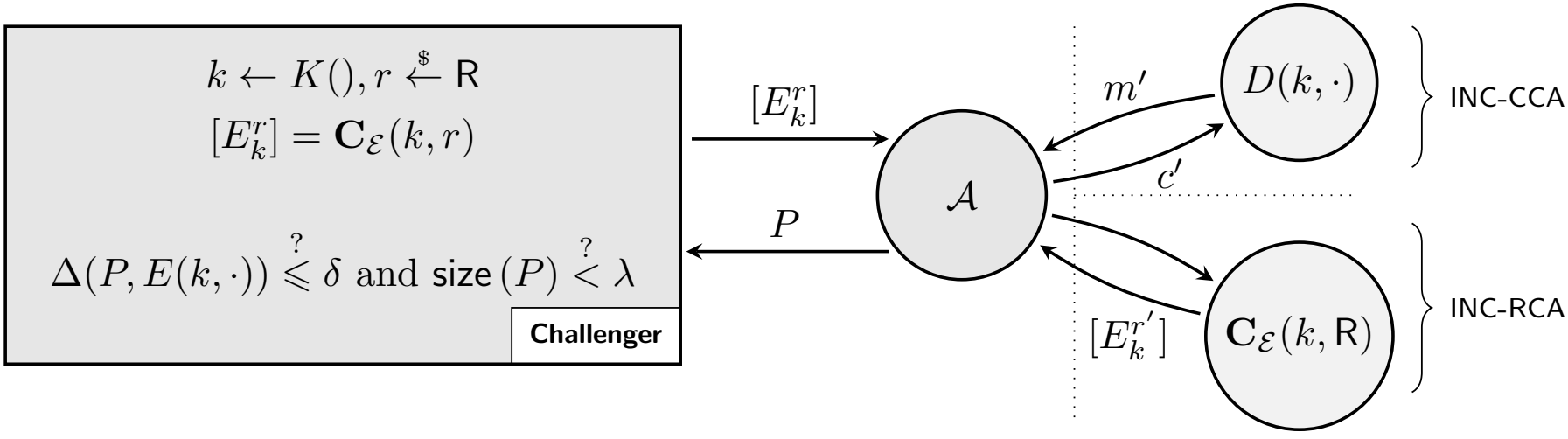


La encore, on peut facilement tester toute hypothèse $\hat{m} = m$.

C'est normal puisque $\mathcal{E}$ est un chiffrement déterministe.

Incompressibilité de programmes (INC)

But: étant donné un programme lourd, en construire un autre équivalent mais beaucoup plus compact



CryptoExperts

Traçabilité des programmes (TRAC)

$\mathbf{C}_{\mathcal{E}}$ possède un **schéma de traçage** si l'on dispose d'un algorithme `trace` qui trace les traîtres:

- on génère une clé $k \xleftarrow{\$} \mathrm{K}$ et $P_1 = [E_k^{r_1}], \ldots, P_n = [E_k^{r_n}]$
- l'adversaire $\mathcal{A}$ obtient $\{P_i, i \in T\}$ pour $T \subseteq [1, n]$
- $\mathcal{A}$ fabrique un programme pirate $Q \leftarrow \mathcal{A}(\{P_i, i \in T\})$
- on arrive à tracer au moins un traître $t \leftarrow \mathtt{trace}(Q, k, r_1, \ldots, r_n)$
- action envers t

Résumé des propriétés voulues

$\alpha \Leftarrow \beta$: si β peut être cassée, α peut l'être aussi

$$\begin{array}{ccccc} \mathsf{INC} & \Leftarrow & \mathsf{UBK} & \Rightarrow & \mathsf{TRAC} \\ & & \Downarrow & & \\ & & \mathsf{OW} & & \end{array}$$

La propriété de base est UBK.

On ne sait pas faire des compilateurs prouvés résistants pour $\mathcal{E} = AES \ldots$

Aperçu

Et en pratique, sait-on faire?

Oui...

- des solutions commerciales existent depuis longtemps sur les segments DRM et pay-TV
- la montée du paiement sur mobile crée un besoin immédiat
- le règlement eIDAS ouvre la voie à la signature numérique sans secure element et commence à exiger des solutions

... et non!

- Nouvelles approches scientifiques pour attaquer des implémentations existantes
- Differential Computation Analysis – BP Award @CHES 2016
- Montée d'expertise des CESTIs

La white-box crypto est un exercice d'engineering contre le hacking opérationnel

Le WhibOx Contest

CryptoExperts
WE INNOVATE TO SECURE YOUR BUSINESS

TU/e

ECRYPT CSA

Go to Dashboard

Call for participation

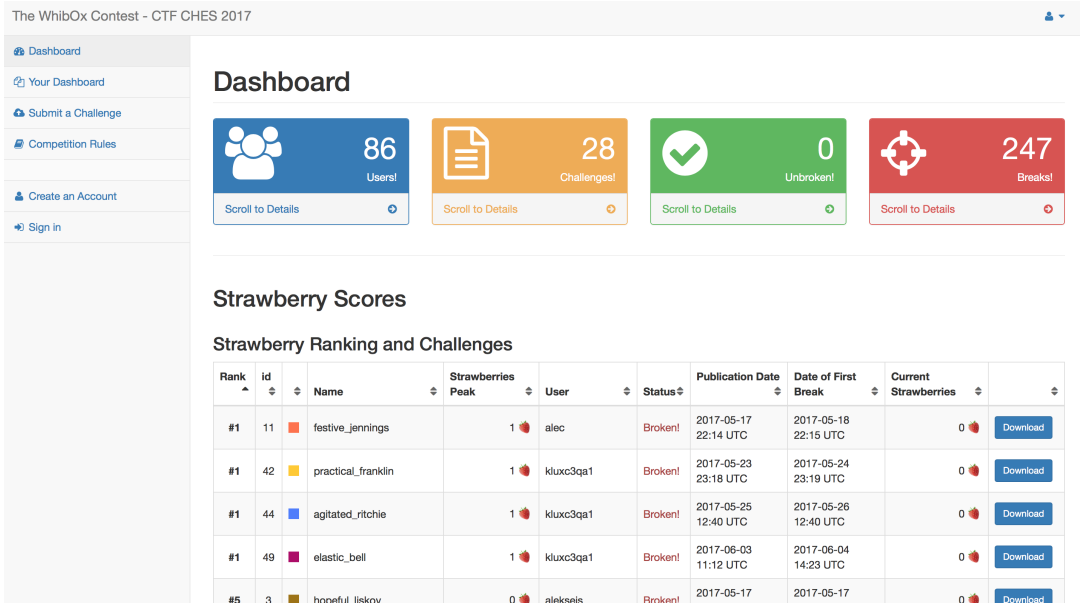
The competition comes in two flavors for competitors:

- Developers are invited to post challenge programs that are white-box implementations of AES-128 under freely chosen keys. Challenges are expected to resist key extraction against a white-box attacker.
- Attackers are invited to break the submitted challenges i.e. extract their hard-coded encryption key.

Participants may remain completely anonymous or use their real-life identity, as they prefer. Implementers are not expected to explain their designs: they only have to provide a resulting C code. Attackers are not expected to explain their techniques: they only have to recover and provide the embedded key(s).

Why this competition?

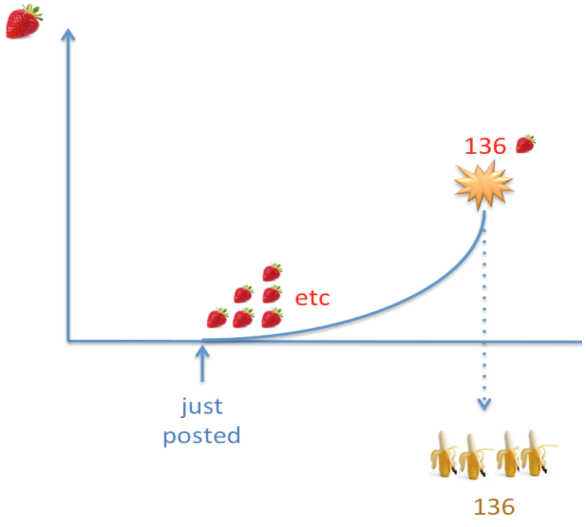
The motivation for initiating the WhibOx contest comes from the growing interest of the industry towards white-box cryptography (most particularly for DRMs and mobile payments) and the obvious difficulty of designing secure solutions in a scientifically valid sense. The conjunction of these phenomena has prompted some companies to develop home-made solutions (with a security



Rank	id		Name	Strawberries Peak	User	Status	Publication Date	Date of First Break	Current Strawberries	
#1	11		festive_jennings	1	alec	Broken!	2017-05-17 22:14 UTC	2017-05-18 22:15 UTC	0	Download
#1	42		practical_franklin	1	kluxc3qa1	Broken!	2017-05-23 23:18 UTC	2017-05-24 23:19 UTC	0	Download
#1	44		agitated_ritchie	1	kluxc3qa1	Broken!	2017-05-25 12:40 UTC	2017-05-26 12:40 UTC	0	Download
#1	49		elastic_bell	1	kluxc3qa1	Broken!	2017-06-03 11:12 UTC	2017-06-04 14:23 UTC	0	Download
#5	3		hopeful_liskov	0	aleksejs	Broken!	2017-05-17	2017-05-17	0	Download

CryptoExperts

Le WhibOx Contest



Banana Scores

Banana Ranking

Rank	User	Bananas
#1	RonaldRietman	1
#1	doegox	1
#1	pschorrhacker	1
#1	SdeH	1
#5	aleksejs	0
#5	olesona	0
#5	Team Megaloblastt	0
#5	OverTime	0
#5	pluto	0
#5	Walter White	0
#5	mlyons3	0
#5	ZetaTwo	0
#5	xanes	0

All Challenge breaks

Date	User	Strawberries	Challenge Name
2017-06-13 05:07 UTC	Nemo	0	stupefied_varahamihira (16)
2017-06-13 04:06 UTC	Nemo	0	quirky_keller (45)
2017-06-13 04:03 UTC	Nemo	0	angry_meitner (7)
2017-06-13 04:01 UTC	Nemo	0	hopeful_liskov (3)
2017-06-12 17:45 UTC	OverTime	0	eloquent_indiana (52)
2017-06-12 15:26 UTC	amberheijden	0	nostalgic_noether (61)
2017-06-12 12:54 UTC	chidoben	0	determined_goldwasser (34)
2017-06-12 08:29 UTC	SdeH	0	happy_yalow (60)
2017-06-12 08:29 UTC	SdeH	0	nostalgic_noether (61)

https://whibox.cr.yp.to

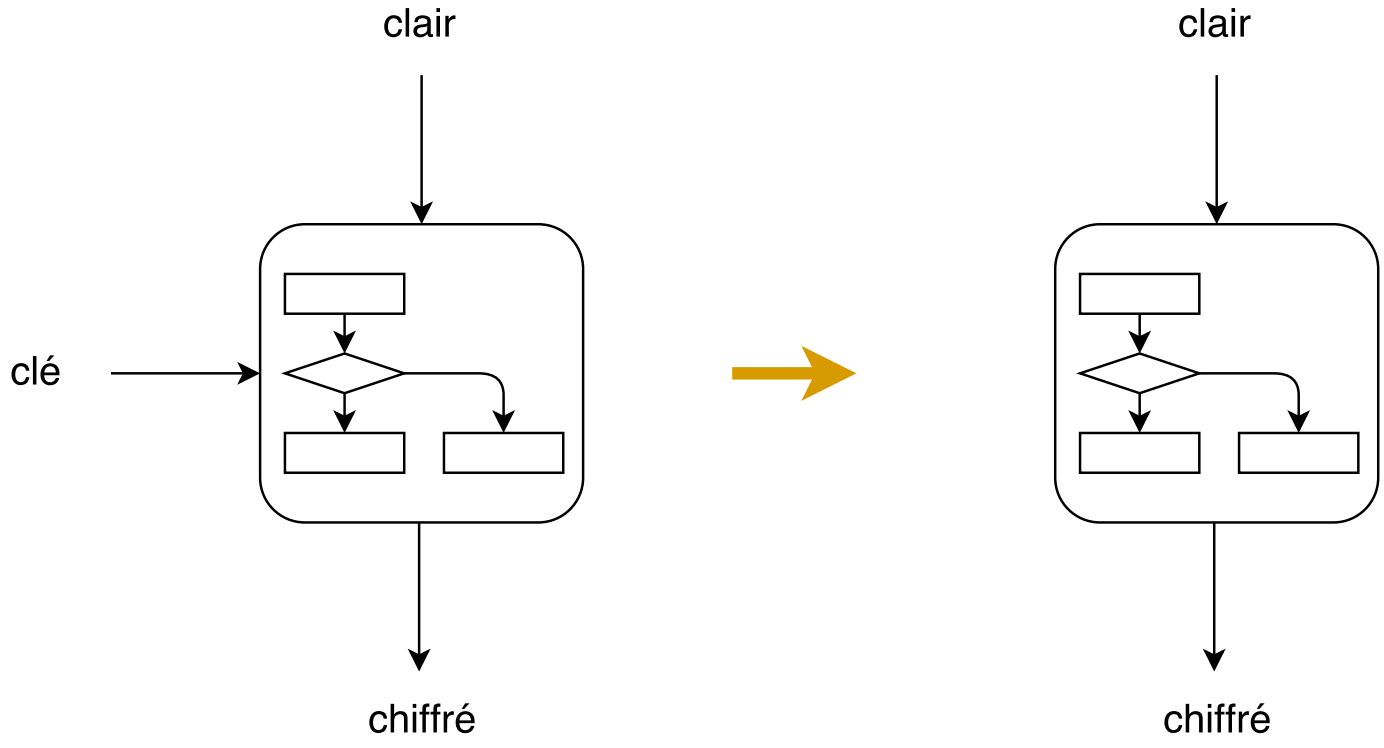
CryptoExperts

Aperçu

CryptoExperts

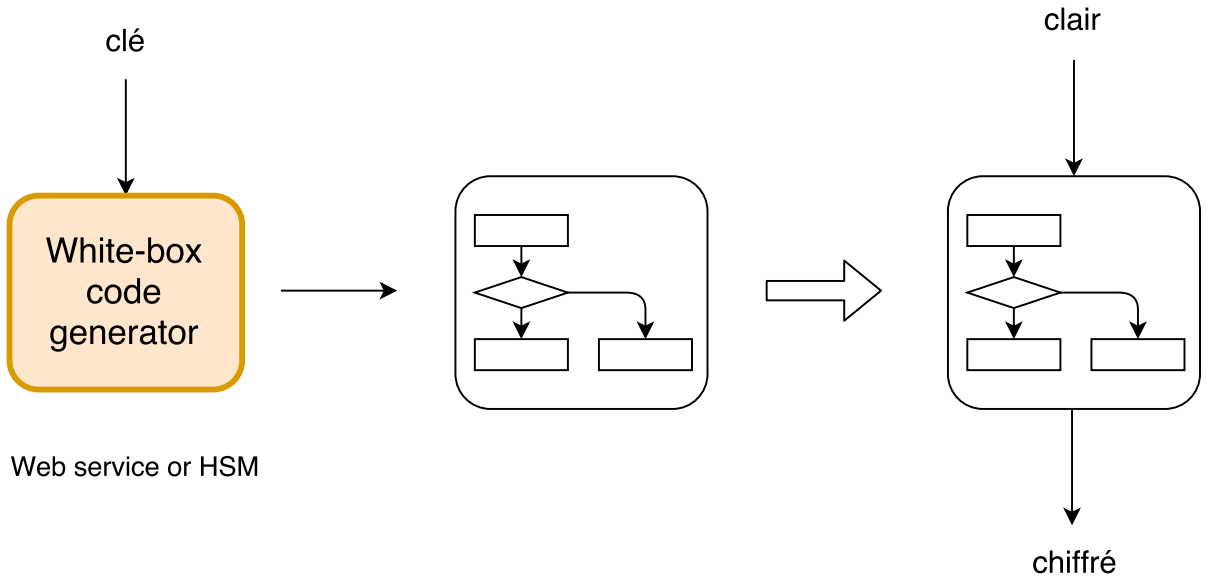
Nos Solutions Opérationnelles

Principe de disparition de la clé



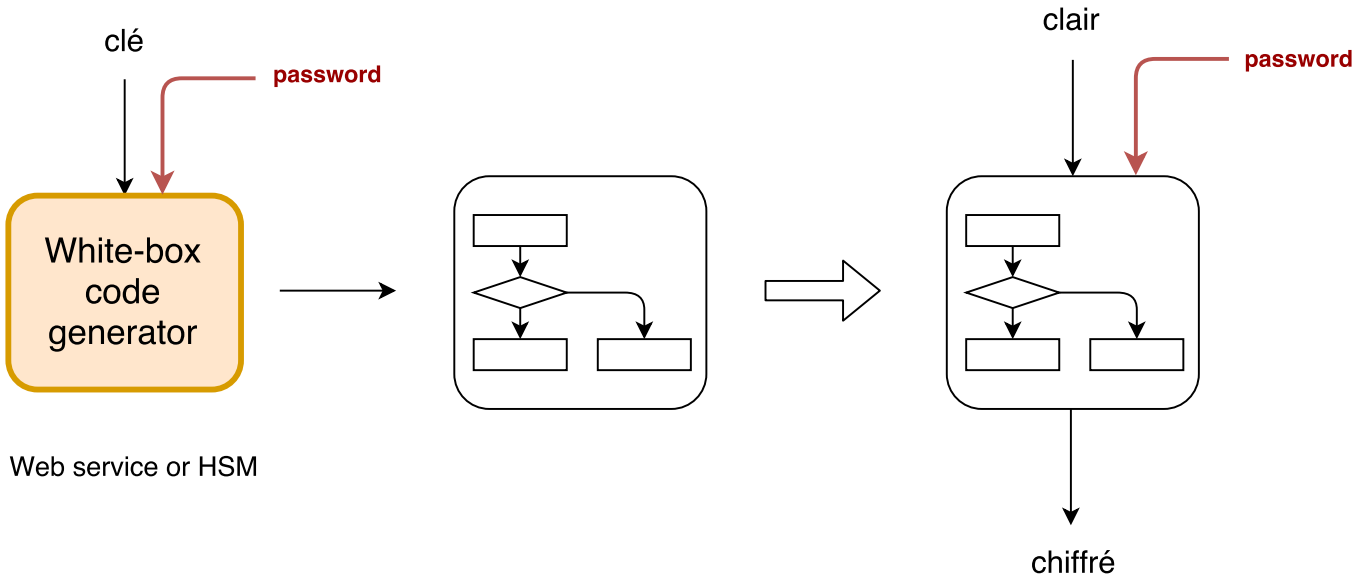
Compilateur Statique

Générateur de programmes en boîte blanche



Compilateur Statique

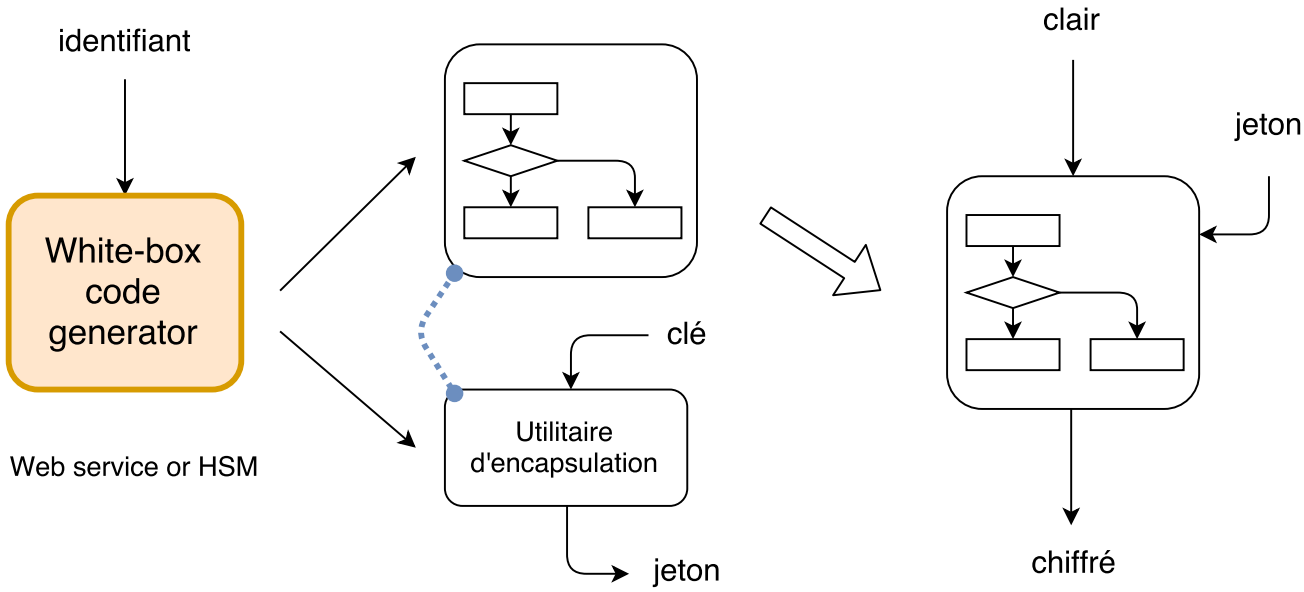
Intégration de protections contre le code lifting



CRYPTOEXPERTS

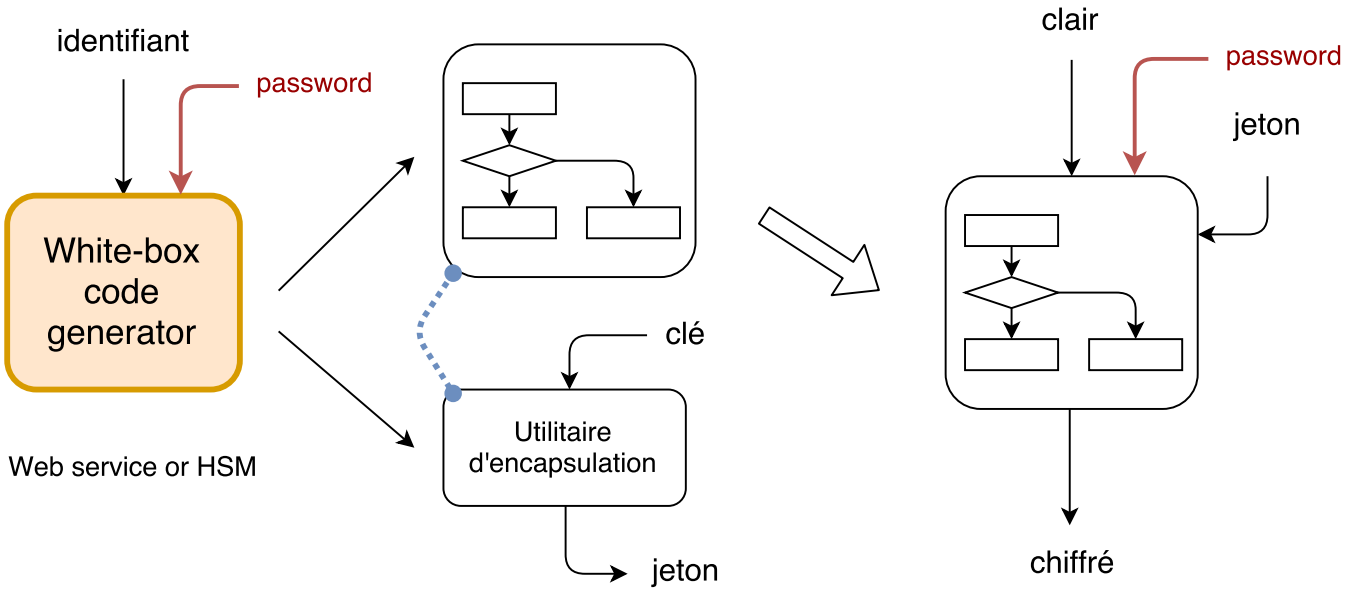
Compilateur Dynamique

La clé peut être renouvelée sans re-déploiement



Compilateur Dynamique

La aussi, protections contre le code lifting



Aperçu

CryptoExperts

Conclusion

La white-box crypto est un paradigme puissant

- des solutions heuristiques mais efficaces existent
- on peut assurer la protection de la clé en pratique
- l'incompressibilité et la traçabilité ont des cas d'usage intéressants

Pour en savoir plus

www.cryptoexperts.com/technologies/white-box

CryptoExperts