non-trivial black-box combiners for collision-resistant hash-functions don’t exist

Krzysztof Pietrzak (CWI Amsterdam)

Eurocrypt May 21 2007

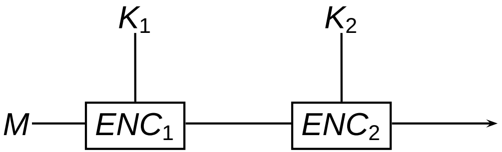
black-box combiners [H05,HKNRR05,PM06,BB06]

C is a secure combiner for XXX[1], if $C^{A,B}$ is a secure implementation of XXX if *either* A or B is a secure implementation of XXX.

[1] put your favorite primitve here

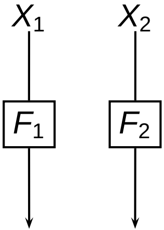
example 1: symmetric encryption

$$C^{ENC_1, ENC_2}([K_1, K_2], M) = ENC_2(K_2, ENC_1(K_1, M))$$



example 2: one way functions

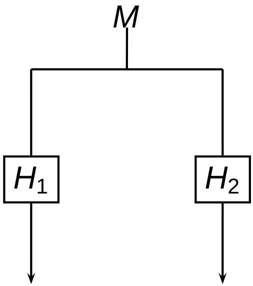
$$C^{F_1,F_2}(X_1, X_2) = F_1(X_1) \| F_2(X_2)$$



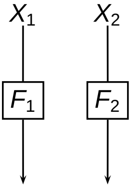
example 3: bike

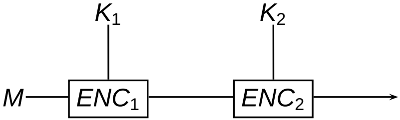
example 4: collision resistant hashing

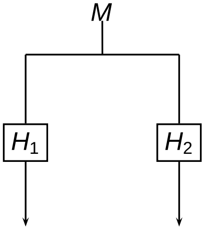
$$C^{H_1,H_2}(M) = H_1(M) \| H_2(M)$$



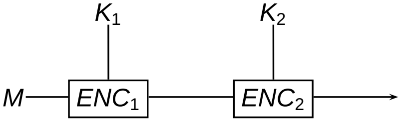
Combined primitives have a twice as large keyspace (ENC,bike), input length (OWF) or output length (OWF & CRHF) compared to the underlying primitive.

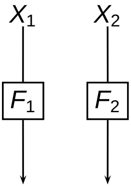


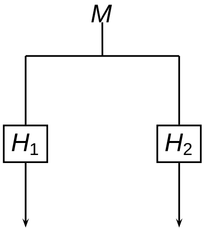




Combined primitives have a twice as large keyspace (ENC,bike), input length (OWF) or output length (OWF & CRHF) compared to the underlying primitive.







do there exist combiners for CRHF with short output?

first try: ignore some bit in the output

- Let
$$C^{H_1,H_2}(M) = H_1(M) \| H_2(M)$$
but with the last output bit removed.

first try: ignore some bit in the output

- Let
$$C^{H_1,H_2}(M) = H_1(M) \| H_2(M)$$
but with the last output bit removed.
- Let $H_1, H_2 : \{0,1\}^* \to \{0,1\}^v$ be uniformly random.

first try: ignore some bit in the output

- Let
$$C^{H_1,H_2}(M) = H_1(M) \| H_2(M)$$
but with the last output bit removed.
- Let $H_1, H_2 : \{0,1\}^* \to \{0,1\}^v$ be uniformly random.
- Let $M \neq M'$ be such that
  1. $C^{H_1,H_2}(M) = C^{H_1,H_2}(M')$
  2. $H_2(M) \neq H_2(M')$ (i.e. they differ in the last bit)

first try: ignore some bit in the output

- Let
$$C^{H_1,H_2}(M) = H_1(M) \| H_2(M)$$
but with the last output bit removed.
- Let $H_1, H_2 : \{0,1\}^* \rightarrow \{0,1\}^v$ be uniformly random.
- Let $M \neq M'$ be such that
    1. $C^{H_1,H_2}(M) = C^{H_1,H_2}(M')$
    2. $H_2(M) \neq H_2(M')$ (i.e. they differ in the last bit)

Such a (M, M') "is of no use" to find a collision for H_2:

$$\begin{aligned} & \Pr[\text{find coll. in } H_2 \text{ given } M, M' \text{ with } q \text{ queries}] \\ = \; & \Pr[\text{ find collision in URF:} \{0,1\}^* \rightarrow \{0,1\}^v] \leq q^2/2^{v+1} \end{aligned}$$

first try: ignore some bit in the output

ignoring even a single bit in

$$C^{H_1,H_2}(M) = H_1(M) \| H_2(M)$$

breaks the combiner completely!

first try: ignore some bit in the output

ignoring even a single bit in

$$C^{H_1,H_2}(M) = H_1(M) \| H_2(M)$$

breaks the combiner completely!

- Maybe there's a more “clever” combiner!

first try: ignore some bit in the output

ignoring even a single bit in

$$C^{H_1,H_2}(M) = H_1(M) \| H_2(M)$$

breaks the combiner completely!

- Maybe there's a more "clever" combiner!
- No, there isn't... But first some definitions.

$$\text{oracle circuit} \quad C : \{0,1\}^m \to \{0,1\}^n$$
$$\text{oracle TM} \quad P : \{0,1\}^{2m} \to \{0,1\}^*$$

$$Adv_P(H_1, H_2, M, M') = \Pr_{P'\text{s coins}}[P^{H_1,H_2}(M, M') \to (X, X', Y, Y'); H_1(X) = H_1(X') \wedge H_2(Y) = H_2(Y')]$$

Definition (BB Combiner for CRHFs)

(C, P) is an ϵ-secure combiner for CRHFs if for all

$$H_1, H_2 : \{0,1\}^* \to \{0,1\}^m$$

and all $M \neq M'$ where

$$C^{H_1,H_2}(M) = C^{H_1,H_2}(M')$$

we have $\quad Adv_P(H_1, H_2, M, M') \geq 1 - \epsilon$

the Boneh-Boyen impossibility result

Theorem (Boneh-Boyen, crypto'06)

For any (C, P)

$$C : \{0,1\}^m \rightarrow \{0,1\}^n \qquad P : \{0,1\}^{2n} \rightarrow \{0,1\}^*$$

where $C^{A,B}$ queries A and B exactly once
if C is shrinking (i.e. $m > n$) and $n < 2v$ then there exist

$$H_1 : \{0,1\}^* \rightarrow \{0,1\}^v \qquad H_2 : \{0,1\}^* \rightarrow \{0,1\}^v$$

and $M \neq M' : C^{H_1,H_2}(M) = C^{H_1,H_2}(M')$ *with*

$$Adv_P(H_1, H_2, M, M') \leq q^2/2^{v+1}$$

Where q is the $\#$ of oracle queries made by P.

more than one query won't help either

Theorem

For any (C, P), *where* C, P *make* q_C, q_P *oracle queries*

$$C : \{0,1\}^m \rightarrow \{0,1\}^n \qquad P : \{0,1\}^{2n} \rightarrow \{0,1\}^*$$

if $m > n$ *and* $n < 2v - 2\log(q_C)$, *then there exist*

$$H_1 : \{0,1\}^* \rightarrow \{0,1\}^v \qquad H_2 : \{0,1\}^* \rightarrow \{0,1\}^v$$

and $M \neq M' : C^{H_1,H_2}(M) = C^{H_1,H_2}(M')$ *with*

$$Adv_P(H_1, H_2, M, M') \leq (q_C + q_P)^2 / 2^{v+1}$$

proof idea

- Have to come up with an oracle $\mathcal{O}$, which on input C comes up with H_1, H_2 and M, M' s.t.
  1. $C^{H_1,H_2}(M) = C^{H_1,H_2}(M')$
  2. given M, M' at least one of the H_i's is a CRHF.

proof idea

- Have to come up with an oracle $\mathcal{O}$, which on input C comes up with H_1, H_2 and M, M' s.t.
  1. $C^{H_1,H_2}(M) = C^{H_1,H_2}(M')$
  2. given M, M' at least one of the H_i's is a CRHF.
- Show that *random* H_1, H_2, M, M' statisfy 1. and 2. with non-zero probability. "satisfying 2." means, that the oracle queries made in the computation of $C^{H_1,H_2}(M), C^{H_1,H_2}(M')$ do not contain collisions for H_1 and H_2.

proof sketch

for $m > n$ and $n < 2v - 2\log(q_C)$ consider any

$$C : \{0,1\}^m \rightarrow \{0,1\}^n$$

For $H_1, H_2 : \{0,1\}^* \rightarrow \{0,1\}^v$ and $M, M' \in \{0,1\}^m$ define the predicates

$$\mathcal{E}_1 \iff C^{H_1,H_2}(M) = C^{H_1,H_2}(M') \wedge M \neq M'$$

$\mathcal{E}_2 \iff$ the computation of $C^{H_1,H_2}(M), C^{H_1,H_2}(M')$ contains collisions for H_1 and H_2.

proof sketch cont.

$$\begin{aligned}\mathcal{E}_1 &\iff C^{H_1,H_2}(M) = C^{H_1,H_2}(M') \wedge M \neq M' \\ \mathcal{E}_2 &\iff \text{computation of } C^{H_1,H_2}(M) = C^{H_1,H_2}(M') \\ &\quad\;\; \text{contains collisions for } H_1 \text{ and } H_2\end{aligned}$$

Lemma (main technical)

For radom H_1, H_2 and M, M' we have $\Pr[\mathcal{E}_1] > \Pr[\mathcal{E}_2]$ and thus $\Pr[\mathcal{E}_1 \wedge \neg\mathcal{E}_2] > 0$

proof sketch cont.

$$\mathcal{E}_1 \iff C^{H_1,H_2}(M) = C^{H_1,H_2}(M') \wedge M \neq M'$$
$$\mathcal{E}_2 \iff \text{computation of } C^{H_1,H_2}(M) = C^{H_1,H_2}(M') \text{ contains collisions for } H_1 \text{ and } H_2$$

Lemma (main technical)

For radom H_1, H_2 *and* M, M' *we have* $\Pr[\mathcal{E}_1] > \Pr[\mathcal{E}_2]$ *and thus* $\Pr[\mathcal{E}_1 \wedge \neg\mathcal{E}_2] > 0$

This implies that there exist H_1, H_2 and M, M' such that $\mathcal{E}_1$ and $\neg\mathcal{E}_2$, i.e. M, M' is a collision for C^{H_1,H_2}, but does not give collisions for H_1 and H_2 (the theorem follows easily from that).

proof sketch of main technical lemma

Lemma (main technical)

For radom H_1, H_2 and M, M' we have $\Pr[\mathcal{E}_1] > \Pr[\mathcal{E}_2]$

Proof.

$\Pr[\mathcal{E}_1] \geq \Pr[C^{H_1,H_2}(M) = C^{H_1,H_2}(M')] - \Pr[M = M'] \geq 2^{-n} - 2^{-m}$

Let $\mathcal{X}_i$ denote the inputs to H_i during the computation of $C^{H_1,H_2}(M), C^{H_1,H_2}(M')$.

$$\Pr[\mathcal{E}_2] = \bigwedge_{i=1,2} \Pr[\exists X \neq X' \in \mathcal{X}_i : H_i(X) = H_i(X')]$$

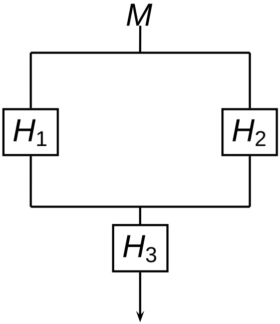
$$\leq \max_{\mathcal{Y}_1,\mathcal{Y}_2,|\mathcal{Y}_1|+|\mathcal{Y}_2|=q_C} \Pr[\prod_{i=1,2} \exists Y \neq Y' \in \mathcal{Y}_i : H_i(X) = H_i(X')]]$$

$$\leq (q_C^2/2^{v+1})^2 < 2^{-n} - 2^{-m} \leq \Pr[\mathcal{E}_1]$$

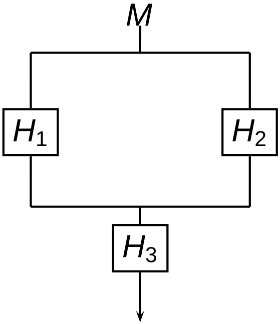
$\square$

if you really want a combiner with short output...

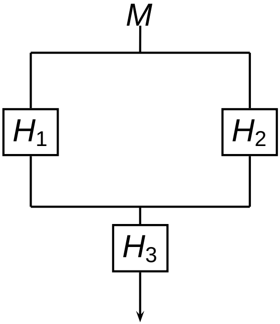
a proposition



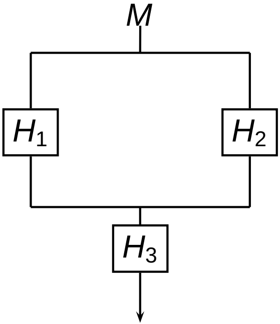
- Secure if H_1 or H_2 and H_3 is a CRHF.



- Secure if H_1 or H_2 and H_3 is a CRHF.
- Seems pointless, if we have to assume that H_3 is secure, why not simply use H_3 to hash M?



- Secure if H_1 or H_2 and H_3 is a CRHF.
- Seems pointless, if we have to assume that H_3 is secure, why not simply use H_3 to hash M?
- In $H_3(H_1(M) \| H_2(M))$, the H_3 is invoked on a short input. So we can use inefficient provably secure H_3.



- Secure if H_1 or H_2 and H_3 is a CRHF.
- Seems pointless, if we have to assume that H_3 is secure, why not simply use H_3 to hash M?
- In $H_3(H_1(M) \| H_2(M))$, the H_3 is invoked on a short input. So we can use inefficient provably secure H_3.
- Say $H_3(a, b) = g^a h^b$ (finding a collision for H_3 is as hard as discrete log).

$$M \longrightarrow g^{H_1(M)} h^{H_2(M)}$$