

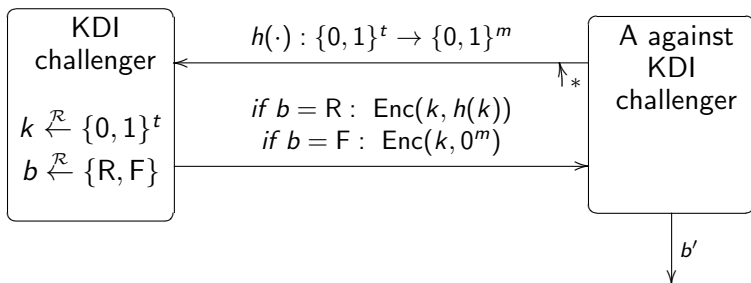
Saarland University
Faculty of Natural Sciences and Technology I
Department of Computer Science
Information Security and Cryptography Group

On the (Im)Possibility of Key Dependent Encryption

Iftach Haitner and Thomas Holenstein

presented by Matthias Berg

Key-dependent input security (KDI) of encryption scheme (Enc, Dec):



(Enc, Dec) is KDI-secure for a class of functions \mathcal{H} , if

$$|\Pr_{k \leftarrow \mathcal{R}} [A^{\text{KDI}_R} = F] - \Pr_{k \leftarrow \mathcal{R}} [A^{\text{KDI}_F} = F]|$$

is negligible for every efficient A that only queries functions in \mathcal{H} .

Hardness Assumptions

A *cryptographic game* is

- a randomized system Γ
- Input: security parameter t
- interacts with an attacker A
- May output a special symbol 'win'

Game Γ is secure, if $\Pr[A(1^t) \leftrightarrow \Gamma(1^t) \text{ wins}]$ is negligible for all PPT A .

Many crypto-proofs use reductions

- A *black-box* reduction of a primitive P (e.g. a KDI-secure encryption scheme) to a primitive Q (e.g. a one-way function) is a construction of P out of Q , where the internal structure of Q is ignored.

Many crypto-proofs use reductions

- A *black-box* reduction of a primitive P (e.g. a KDI-secure encryption scheme) to a primitive Q (e.g. a one-way function) is a construction of P out of Q , where the internal structure of Q is ignored.
- *fully-black-box*: The proof of security is also black-box.
e.g. $\exists A$ breaking $P \Rightarrow \exists B$ breaking Q , where internal structure of A is ignored.

Many crypto-proofs use reductions

- A *black-box* reduction of a primitive P (e.g. a KDI-secure encryption scheme) to a primitive Q (e.g. a one-way function) is a construction of P out of Q , where the internal structure of Q is ignored.
- *fully-black-box*: The proof of security is also black-box.
e.g. $\exists A$ breaking $P \Rightarrow \exists B$ breaking Q , where internal structure of A is ignored.
- *strongly-black-box* reduction to Γ (KDI-specific): Proof of security accesses the query function h in a black-box manner as well. (access to h is also not forwarded to a third party)
 - $\exists A_{\Gamma}^{(\cdot)}. \forall B^{\text{KDI}}$ breaking the KDI-security. $A_{\Gamma}^{(B)}$ violates the security of Γ .

Breaker

- Let t be the security parameter (and the key length)
- Let $l(t)$ be the length encryptions of messages of length $2t$.
- Let $\mathcal{H} = \{h_t : \{0, 1\}^t \rightarrow \{0, 1\}^{2t}\}_{t \in \mathbb{N}}$ chosen at random.

Definition (Algorithm Breaker)

- Input: An index t a function $f : \{0, 1\}^t \times \{0, 1\}^{l(t)} \rightarrow \{0, 1\}^{2t}$ and a ciphertext $c \in \{0, 1\}^{l(t)}$.
- Output smallest $k \in \{0, 1\}^t$ with $f(k, c) = h_t(k)$, or \perp if no such k .

Breaker

- Let t be the security parameter (and the key length)
- Let $l(t)$ be the length encryptions of messages of length $2t$.
- Let $\mathcal{H} = \{h_t : \{0, 1\}^t \rightarrow \{0, 1\}^{2t}\}_{t \in \mathbb{N}}$ chosen at random.

Definition (Algorithm Breaker)

- Input: An index t a function $f : \{0, 1\}^t \times \{0, 1\}^{l(t)} \rightarrow \{0, 1\}^{2t}$ and a ciphertext $c \in \{0, 1\}^{l(t)}$.
- Output smallest $k \in \{0, 1\}^t$ with $f(k, c) = h_t(k)$, or \perp if no such k .

Definition (Algorithm $A_{\text{KDI}}^{\text{Breaker}, \mathcal{H}}$)

- Call $\text{KDI}_?$ on $h_t(\cdot)$ to obtain encryption c of $h_t(k)$ (or of 0^{2t}).
- Call $\text{Breaker}(t, \text{Dec}, c)$ and output 1 if Breaker does not return \perp .

Lemma

$A_{\text{KDI}}^{\text{Breaker}, \mathcal{H}}$ breaks the KDI-security of (Enc, Dec) .

Breaker does not yield additional power

Lemma

Let $A^{\text{Breaker}, \mathcal{H}}$ be an algorithm and let $t_A(n)$ a polynomial upper bound on the running time of $A^{\text{Breaker}, \mathcal{H}}$.

For every $\delta : \mathbb{N} \rightarrow [0, 1]$, there is an algorithm $B^{\mathcal{H}}$ which runs in time $\text{poly}(\frac{1}{\delta(n)}, t_A(n))$ and if $A^{\text{Breaker}, \mathcal{H}}$ and $B^{\mathcal{H}}$ use the same random coins, then $\Pr_{\mathcal{H}}[A^{\text{Breaker}, \mathcal{H}}(1^n) = B^{\mathcal{H}}(1^n)] \geq 1 - \delta(n)$

Breaker does not yield additional power

Lemma

Let $A^{\text{Breaker}, \mathcal{H}}$ be an algorithm and let $t_A(n)$ a polynomial upper bound on the running time of $A^{\text{Breaker}, \mathcal{H}}$.

For every $\delta : \mathbb{N} \rightarrow [0, 1]$, there is an algorithm $B^{\mathcal{H}}$ which runs in time $\text{poly}(\frac{1}{\delta(n)}, t_A(n))$ and if $A^{\text{Breaker}, \mathcal{H}}$ and $B^{\mathcal{H}}$ use the same random coins, then $\Pr_{\mathcal{H}}[A^{\text{Breaker}, \mathcal{H}}(1^n) = B^{\mathcal{H}}(1^n)] \geq 1 - \delta(n)$

Theorem

There exists no reduction with strongly-black-box proof of security from a KDI encryption scheme to any secure hardness assumption Γ .

Theorem

There exists no fully-black-box reduction from an encryption scheme that is KDI-secure against every poly(n)-wise independent family of hash functions to one-way permutations.

Thank You!