Ciphers that Securely Encipher their own Keys
ECS 227 Paper Writeup

Mar 20, 2012

Sisi Duan

Main Result

The goal of the paper, due to Bellare, Cash, and Keelveedhi, is to provide *efficient* tweakable ciphers that are proven to securely encipher their own keys. Specifically, they proposed a narrowblock design(data is n bits long where n is the block length) **StE** (based on XEX [5]) and a wideblock design(data is mn bits long for $m \geq 2$) **EtE** (based on [4]).

Conventional Symmetric-Key Encryption

The security notions of a conventional symmetric-key encryption that we usually consider are IND-CPA (or stronger IND-$) security (in terms of chosen-plaintext attack), and IND-CCA (or stronger AE) security (in terms of chosen-plaintext attack). The schemes to achieve them have to be randomized or stateful. In other words, the length of a ciphertext has to be longer than its corresponding plaintext.

But there are applications which asks for length-preservation like disk encryption. In such scenario, we consider using *ciphers*. Cipher is a family of deterministic, length preserving permutations over the message space. For example, AES is considered to be a "good" cipher. We use the notion $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ to represent a typical blockcipher in class. The security notions are PRP and strong PRP (SPRP, or PRP-CCA). A tweakable blockcipher is a map $E : \{0,1\}^k \times \mathcal{T} \times \{0,1\}^m \to \{0,1\}^m$ that takes input a k-bit key K, a tweak T drawn from the tweakspace $\mathcal{T}$ and a m-bit message M to return an m-bit output $E(K,T,M)$. The security notions are tweakable PRP-CPA or tweakable PRP-CCA.

In this writeup, we consider *both* the conventional symmetric-key encryption and cipher.

Encryptions and Ciphers in the presence of Key-Dependent Messages

The above-mentioned notions for encryption and cipher are *not* adequate for circumstances where one encrypts messages that depends on the underlying secret key. We call the new notion as KDM security.

This is desirable in some areas such as disk encryption conducted by the Security in Storage Working Group (IEEE P1619). The KDM security notions can be applied to ciphers, symmetric key encryption and even public key encryption. For example, Camenisch and Lysyanskaya use KDM secure public key encryption to construct anonymous credential (which is not the focus of this writeup).

This paper focus on a specific case of cipher that encrypts the key and I would like to focus on the symmetric key setting in this writeup.

Key-Dependent Messages (KDM)

KDM refers to an attack model that allows requested plaintexts to depend on the underlying decryption key. It is a very strong definition of security that allows the adversary indirect access to hidden keys. I would like to show the notion of symmetric KDM security under the standard model. For the notion of KDM security in the public-key setting, please refer [2].

KDM Secure Encryption. Similar with IND-CPA notion, the notion of IND-KDM security defines two experiments, **Real** and **Fake**. Initially, a vector of keys $\mathbf{K} = (K_1, K_2, \cdots)$. **For** $i \in \{1, 2, \cdots\}$ **do** $K_i \overset{\$}{\leftarrow} \mathcal{K}$.

- Real: The $\mathsf{Real}_{\mathbf{K}}$ takes input $j \in \{1, 2, \cdots\}$ and a function g that maps $\mathbf{K} \in (\{0,1\}^*)^\infty$ to $g(\mathbf{K}) \in \{0,1\}^*$, probabilistically encrypts $M = g(\mathbf{K})$ under key K_j.

- Fake: The $\mathsf{Fake}_{\mathbf{K}}$ takes input j and g, probabilistically encrypts $|g(\mathbf{K})|$ zero-bits under key K_j.

Definition 1 (IND-KDM - standard model-symmetric setting)**.** *Let* $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ *be a symmetric encryption scheme and let A be an adversary. For* $\boldsymbol{K} \in (\{0,1\}^*)^\infty$*, let*

$\mathit{Real}_{\mathbf{K}}$ *be the oracle that on input* (j, g) *returns* $C \overset{\$}{\leftarrow} \mathcal{E}_{K_j}(g(\mathbf{K}))$ *and let*

$\mathit{Fake}_{\mathbf{K}}$ *be the oracle that on input* (j, g) *returns* $C \overset{\$}{\leftarrow} \mathcal{E}_{K_j}(0^{|g(\mathbf{K})|})$

$\mathit{Adv}^{kdm}_{\Pi}(A) \overset{def}{=} |Pr[\mathbf{K} \overset{\$}{\leftarrow} \mathcal{K} : A^{\mathit{Real}_{\mathbf{K}}} = 1] - Pr[\mathbf{K} \overset{\$}{\leftarrow} \mathcal{K} : A^{\mathit{Fake}_{\mathbf{K}}} = 1]|$

A Caveat. Note that this definition is described in a way that a sector of keys are involved which we call the multi-user setting. Indeed, it seems to entail a loss of generality by just assuming one single key. An interesting example one usually consider in the reference is to circularly encrypt keys, i.e. $E_{K_1}(K_2), E_{K_2}(K_3), \cdots, E_{K_n}(K_1)$.

Also this is not a problem for a conventional encryption, since single-user setting security implies multi-user setting security (using hybrid argument).

Random Oracle Based Definition. It is proved in paper [2] that there exists a KDM-secure randomized encryption scheme in the random oracle model, which is defined in the following.

Definition 2 (IND-KDM - RO model-symmetric setting)**.** *Let* $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ *be a symmetric encryption scheme for the RO model, and let A be an adversary. For* $\boldsymbol{K} \in (\{0,1\}^*)^\infty$*, let*

$\mathit{Real}_{\mathbf{K}}$ *be the oracle that on input* $(j, g^?)$ *returns* $C \overset{\$}{\leftarrow} \mathcal{E}^H_{K_j}(g^H(\mathbf{K}))$ *and let*

$\mathit{Fake}_{\mathbf{K}}$ *be the oracle that on input* $(j, g^?)$ *returns* $C \overset{\$}{\leftarrow} \mathcal{E}^H_{K_j}(0^{|g^H(\mathbf{K})|})$

$\mathit{Adv}^{kdm}_{\Pi}(A) \overset{def}{=} |Pr[\mathbf{K} \overset{\$}{\leftarrow} \mathcal{K}, H \overset{\$}{\leftarrow} \Omega : A^{\mathit{Real}_{\mathbf{K}}} = 1] - Pr[\mathbf{K} \overset{\$}{\leftarrow} \mathcal{K}, H \overset{\$}{\leftarrow} \Omega : A^{\mathit{Fake}_{\mathbf{K}}} = 1]|$

KDM Secure Cipher. This paper does not use random oracles while still proves KDM secure PRPs. To be specific, this paper defines and focus on Φ-PRP-CCA security where Φ is a class of functions that map n-bit keys to mn-bit inputs. Φ is an arbitrary function in the definition of security notions, when it comes into the construction the author in [1] only consider Φ as an identity function. (This is in light of the negative result from [3] and due to the consideration of efficiency and, of course, the application driven.) Here we slightly deviate the definition from [1] for consistency.

Definition 3 (Φ-KDM-PRP-CCA - standard model)**.** *Let* $E : \{0,1\}^k \times \mathcal{T} \times \{0,1\}^m \to \{0,1\}^m$ *be a tweakable blockcipher and let A be the adversary. Let* $Perm(\mathcal{T}, n)$ *be the set of all mappings from* $\mathcal{T}$ *to permutations on n bits. Let*

$\mathit{Real}_{\mathbf{K}}$ *be the oracle that on input* (T, ϕ) *returns* $C \overset{\$}{\leftarrow} E(K, T, \phi(K))$ *and let*

$\mathit{Fake}_{\mathbf{K}}$ *be the oracle that on input* (T, ϕ) *returns* $C \overset{\$}{\leftarrow} \pi(T, \phi(K))$

$\mathit{Adv}^{prp-cca}_{E,\Phi}(A) = Pr[K \overset{\$}{\leftarrow} \mathcal{K} : A^{E(\cdot,\cdot), E^{-1}(\cdot,\cdot), \mathit{Real}_K} = 1] - Pr[\pi \overset{\$}{\leftarrow} Perm(\mathcal{T}, n), A^{\pi(\cdot,\cdot), \pi^{-1}(\cdot,\cdot), \mathit{Fake}_K} = 1].$

where, above, the adversary A is not allowed to deciphering query with (T, C) for C previously received from the key dependent function oracle.

A Narrowblock Cipher Construction

First, the authors construct a narrowblock tweakable blockcipher **StE** that can securely encipher its own key. Let $E : \{0,1\}^k \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ be a tweakable blockcipher that has the same key length and message length n. Fix an arbitrary tweak $\gamma \in \mathcal{T}$ and an arbitrary message $\alpha \in \{0,1\}^n$. Both γ and α are public parameters known to the adversary. The scheme transforms $\mathbf{StE}_{\gamma,\alpha}$ to another tweakable blockcipher $F = \mathbf{StE}_{\gamma,\alpha}[E] : \{0,1\}^n \times \mathcal{T}\backslash\{\gamma\} \times \{0,1\}^n \to \{0,1\}^n$. The function F and F^{-1} are defined as follows:

```
$F(K, T, M)$
01 $H \leftarrow E(K, \gamma, \alpha)$
02 If $M = K$ then $Y \leftarrow E(K, T, H)$
03 Else If $M = H$ then $Y \leftarrow E(K, T, K)$
04 Else $Y \leftarrow E(K, T, M)$
05 Return $Y$
```

```
$F^{-1}(K, T, C)$
01 $Y \leftarrow D(K, T, C)$
02 $H \leftarrow E(K, \gamma, \alpha)$
03 If $Y = K$ then $M \leftarrow H$
04 Else If $Y = H$ then $M \leftarrow K$
05 Return $M$
```

Security Intuition. To sketch the proof of **StE**. The only line that encrypt the key K is the third line, where M equals H, which is very unlikely and named “hidden” point in the paper. The reason comes from the fact that H is the encryption of K, γ, and α and the restriction that the tweak γ is removed from the oracle of the adversary.

References

[1] M. Bellare, D. Cash, and S. Keelveedhi. *Security amplification by composition: The case of doubly-iterated, ideal ciphers*, ACM Conference on Computer and Communications Security 2011: 423-432.

[2] J. Black, P. Rogaway, and T. Shrimpton. *Encryption-Scheme Security in the Presence of Key-Dependent Messages.* Selected Areas in Cryptography 2002 (SAC 2002), LNCS vol. 2595, pp. 62-75, Springer, 2002.

[3] S. Halevi and H. Krawczyk. Security under Key-Dependent Inputs. 14th ACM-CCS, pages 466-475, 2008. ACM.

[4] S. Halevi and P. Rogaway. A Parallelizable Enciphering Mode. Topics in Cryptology, CT-RSA 2004, LNCS vol. 2964, pp. 292-304, Springer, 2004.

[5] Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. Phillip Rogaway. Asiacrypt 2004. LNCS vol. 3329. Springer, 2004.