Encryption Schemes Secure under Related-Key and Key-Dependent Message Attacks

Florian Böhl, Gareth T. Davies and Dennis Hofheinz
gareth.davies@bristol.ac.uk

Karlsruhe Institute of Technology and University of Bristol

PKC '14

28 March 2014

KDM Security in the Hybrid Framework

Results

Context

Investigated the joint security of related-key and key-dependent message attacks:

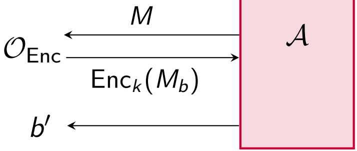
- Present a number of schemes secure under RKA-KDM.
- Provide a generic framework for proving schemes secure under the notion.

Chosen Plaintext Attack Security

Before we define KDM and RKA security, first recall the definition of IND-CPA security (symmetric encryption):

$$b \in \{0,1\}$$
$$k \leftarrow \{0,1\}^*$$

$$\boxed{\begin{aligned} M_1 &= M \\ M_0 &= 0^{|M|} \end{aligned}}$$



$\mathcal{A}$ wins if $b' = b$, and the scheme is IND-CPA-secure if $\mathcal{A}$'s advantage is no better than guessing.

Key-Dependent Message Security

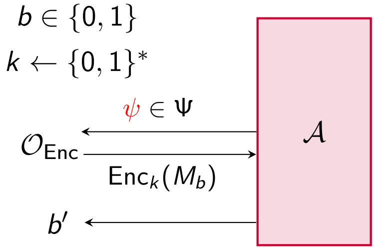
Key-Dependent Message (KDM) Security involves an environment where the **adversary can receive encryptions of arbitrary functions of the secret key**, and it is a concern in many scenarios:

- Disk encryption systems (e.g. Bitlocker)
- Anonymous Credential Systems
- Formal Verification (Dolev-Yao proofs)

Key-Dependent Message Security

Now to define KDM security (symmetric setting):

$$\boxed{\begin{aligned} M_1 &= \psi(k) \\ M_0 &= 0^{|\psi(k)|} \end{aligned}}$$



Scheme is KDM-CPA[Ψ] Secure if $\mathcal{A}$'s advantage is no better than guessing.

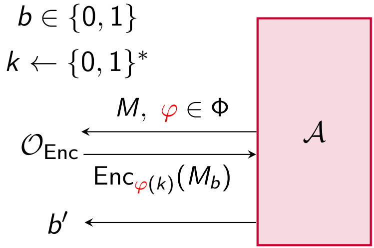
Prior Work in KDM Security

- Camenisch and Lysyanskaya EC'01 (anonymous credential systems) & Black, Rogaway and Shrimpton SAC'02 (definitions in ROM).
- Boneh et al. Crypto'08 presented the first scheme secure under chosen plaintext attacks in the standard model.
- Camenisch et al. EC'09 gave a scheme secure under active attacks in the standard model.
- Numerous schemes KDM-secure under a variety of number-theoretic assumptions.
- Negative results suggesting difficulty of acquiring generic statements.

Definition of Related-Key Attack Security

Now to define RKA security (symmetric setting):

$$\boxed{\begin{aligned} M_1 &= M \\ M_0 &= 0^{|M|} \end{aligned}}$$



Scheme is RKA[Φ] Secure if $\mathcal{A}$'s advantage is no better than guessing.

Why RKA-KDM Security?

- Desirable to have modular approach to security notions including scope to introduce further notions.
- Combine two interesting and active research areas.

Applebaum TCC'13 first introduced the joint notion

§ In context of getting XOR "for free" in garbled circuit constructions using RKA-KDM secure schemes.

§ Showed RKA security + KDM security $\not\Rightarrow$ RKA-KDM security.

§ Gave a scheme secure under LPN as proof of concept.

Definition of RKA-KDM Security

RKA-KDM security (symmetric setting):

$b \in \{0,1\}$

$k \leftarrow \{0,1\}^*$

$$\boxed{\begin{array}{l} M_1 = \psi(k) \\ M_0 = 0^{|\psi(k)|} \end{array}}$$

$$\mathcal{O}_{\mathsf{Enc}} \xleftarrow{\varphi \in \Phi,\ \psi \in \Psi} \mathcal{A}$$

$$\mathcal{O}_{\mathsf{Enc}} \xrightarrow[\mathsf{Enc}_{\varphi(k)}(M_b)]{} \mathcal{A}$$

$$b' \longleftarrow \mathcal{A}$$

Scheme is RKA-KDM$[\Phi, \Psi]$ Secure if $\mathcal{A}$'s advantage is no better than guessing.

Generic Framework for RKA-KDM secure encryption

To achieve RKA-KDM secure encryption, we reduce the scheme in question to three properties:

- IND-CPA security
- Existence of oracle that, given an RKA function φ and a (valid) encryption of M under key k, outputs $\mathsf{Enc}_{\varphi(k)}(M)$.
- Existence of oracle that, given a KDM function ψ and a (valid) encryption of M under key k, outputs $\mathsf{Enc}_k\big(\psi(k)\big)$.

We modify the following schemes to yield provably RKA-KDM secure symmetric schemes:

- § Boneh et al. (BHHO) Crypto08 under DDH
- § Applebaum et al. (ACPS) Crypto09 under LWE
- § Brakerski & Goldwasser Crypto10 under DDH + QR
- § Bellare et al. (BHR) CCS 2012
- § Malkin et al. (MTY) EC11 under DCR

Variant of the BHHO scheme

Group $\mathbb{G}$ of prime order p, generators $g, g_1, .., g_\lambda$ and $M \in \{0, 1\}$.

Variant of the BHHO scheme

Group $\mathbb{G}$ of prime order p, generators $g, g_1, .., g_\lambda$ and $M \in \{0, 1\}$.

- KeyGen: $k = (k_1, \ldots, k_\lambda) \leftarrow \{0, 1\}^\lambda$.

Variant of the BHHO scheme

Group $\mathbb{G}$ of prime order p, generators $g, g_1, .., g_\lambda$ and $M \in \{0,1\}$.

- KeyGen: $k = (k_1, \ldots, k_\lambda) \leftarrow \{0,1\}^\lambda$.
- Enc(M): pick $r_1, \ldots, r_\lambda \leftarrow \mathbb{Z}_p$ and set $g_0 := \prod_{i \in [\lambda]} (g_i^{r_i})^{-k_i}$, then return

$$C := (g_1^{r_1}, \ldots, g_\lambda^{r_\lambda}, g^M \cdot g_0).$$

Variant of the BHHO scheme

Group $\mathbb{G}$ of prime order p, generators $g, g_1, .., g_\lambda$ and $M \in \{0,1\}$.

- KeyGen: $k = (k_1, \ldots, k_\lambda) \leftarrow \{0,1\}^\lambda$.
- Enc(M): pick $r_1, \ldots, r_\lambda \leftarrow \mathbb{Z}_p$ and set $g_0 := \prod_{i \in [\lambda]} (g_i^{r_i})^{-k_i}$, then return
$$C := (g_1^{r_1}, \ldots, g_\lambda^{r_\lambda}, g^M \cdot g_0).$$
- Dec(C): Parses C as $(x_1, \ldots, x_\lambda, y)$.
Computes $\tilde{M} := y \cdot \prod_{i \in [\lambda]} x_i^{k_i}$.
Returns 0 if $\tilde{M} = 1$, returns 1 if $\tilde{M} = g$, otherwise returns $\perp$.

RKA Oracle

RKA function class $\varphi \in \Phi : k \mapsto k \oplus \Delta$.

Require that oracle doesn't require k yet still outputs an encryption under related key $k \oplus \Delta$ when given valid ciphertext:

RKA Oracle

RKA function class $\varphi \in \Phi : k \mapsto k \oplus \Delta$.

Require that oracle doesn't require k yet still outputs an encryption under related key $k \oplus \Delta$ when given valid ciphertext:

- Given $C = (x_1, \ldots, x_\lambda, y)$ and φ_Δ, compute:

$$C' := (x_1^{(-1)^{\Delta_1}}, \ldots, x_\lambda^{(-1)^{\Delta_\lambda}}, y \cdot \prod_{i \in [\lambda]} x_i^{\Delta_i})$$

KDM Oracle

KDM Function class $\psi \in \Psi : k \mapsto k_i \oplus b$.

Require that oracle doesn't require k yet still outputs encryption of $k_i \oplus b$ under k:

KDM Oracle

KDM Function class $\psi \in \Psi : k \mapsto k_i \oplus b$.

Require that oracle doesn't require k yet still outputs encryption of $k_i \oplus b$ under k:

- Given an honestly generated ciphertext of b denoted $C = (x_1, \ldots, x_\lambda, y)$ and $\psi_{i,b}$, compute:

$$C' := (x_1, \ldots, x_{i-1}, x_i \cdot g^{(-1)^b}, x_{i+1}, \ldots, x_\lambda, y)$$

Conclusions

Presented a generic framework for constructing RKA-KDM secure symmetric encryption schemes, and provided examples of adaptations of known KDM-secure schemes.

Full version: ePrint 2013/653.

Thanks for your attention!

Questions?