Key Dependent Message Security: Recent Results and Applications

Tal Malkin
Columbia University
tal@cs.columbia.edu

Isamu Teranishi
NEC Corporation
Columbia University
teranisi@ah.jp.nec.com

Moti Yung
Google Inc.
Columbia University
moti@cs.columbia.edu

ABSTRACT

An encryption scheme is *Key Dependent Message (KDM) secure* if it is secure even against an attacker who has access to encryptions of messages which depend on the secret key. Recent studies have revealed that this strong security notion is important both theoretically and practically. In this paper we review the definition, and survey recent results and applications of KDM security.

Categories and Subject Descriptors

C.2.0 [**COMPUTER-COMMUNICATION NETWORKS**]: General—*Security and protection*; K.4.4 [**COMPUTERS AND SOCIETY**]: Electronic Commerce—*Security*; D.4.6 [**Software**]: OPERATING SYSTEMS—*Security and Protection*

General Terms

Security, Cryptography, Encryption

Keywords

Key Dependent Message Security, KDM, Circular Encryption, Survey

1. INTRODUCTION

The design of public key systems that are secure against attackers which are given a class of functons, and are allowed to request ciphertexts that are each a chosen function (from the given class) of the system's secret keys is a very active area of research. The initial schemes designed in this area were called "circular" [17] and allowed encryption of a secret key or a linear function of a secret key. Later on, more general functions were considered and the security of these schemes was called *Key Dependent Message (KDM) security* [11]. In particular, we say that a public-key encryption (PKE) scheme is *KDM*[$\mathcal{F}$] *secure* (where $\mathcal{F}$ is a class of functions), if it is secure even against an adversary who is given public keys $\mathrm{pk}_1, \ldots, \mathrm{pk}_n$ and has access to encryptions of key dependent messages $f(\mathrm{sk}_1, \ldots, \mathrm{sk}_n)$ for adaptively selected functions $f \in \mathcal{F}$.

Originally motivated by the fact that in some systems, keys encrypt other keys (by design or by misuse of protocols), recent research has revealed sdditional important motivation for studying KDM security. On the theoretical side, KDM security can be used to "reconcile" the two fundamental views of security, indistinguishability-based security and Dolev-Yao security [1, 11, 3, 7]. This notion also has surprising connections with other fundamental notions: cryptographic agility [2], obfuscation [18], and encryption with weakly random keys [18]. On the practical side, KDM security is crucial for designing some recent cryptographic protocols. For instance, this notion is used in an anonymous credential system [17], where a KDM secure encryption is used to discourage delegation of credentials. Another example is fully homomorphic encryption, where KDM security is used to achieve the full unbounded construction of [20]. KDM security is also used in the applied case of arguing the security of disk encryption utilities [12] where the disc encryption key may end up being stored in the page files and thus is encrypted along with the disc content.

CODASPY'11, February 21–23, 2011, San Antonio, Texas, USA.

2. HISTORY OF KDM SECURITY

In this section we briefly overview the history of the KDM security definitions and results. We provide more details (in particular, regarding the technical aspects of these works) in later sections.

2.1 Prehistory of KDM Security

Cryptographers traditionally thought of this kind of "self-encryption" as a dangerous abuse of an encryption scheme. For instance, the seminal work of Goldwasser and Micali [22] already observed that semantic security may not hold if an adversary gets to see an encryption of the secret key.

Another example of a group who considered self-encryption as abuse are the members of the IEEE P1619 standard group [31, 32]. When this group was developing a standard for sector level encryption, they discussed an attack on the tweakable cipher of [29] using self-encryption, and argued whether this self-encryption is a real problem or just a theoretical possibility. They then found that the implementation of disk encryption in Windows Vista$^{\mathrm{TM}}$ stored this kind of self-encryption on the disk in some situations. Consequently, they switched to a different scheme based on [37]. Note that, after that event, self-encryptions of tweakable cipher was extensively studied in [26].

2.2 Proposing the KDM Security Notion

Positive aspects of self-encryption were first studied by Camenisch and Lysyanskaya [17] and independently by Black, Rogaway, and Shrimpton [11]. In [17] it was realized that self-encryption could be used to discourage delegation of credentials in the setting of anonymous credential systems. They then formalized the security of self-encryption, called this security notion *circular security*, and proposed circular secure encryption based on the random oracle model.

On the other hand, the authors of [11] studied self-encryption in a different context. Their motivation came from the progress in studies of the Dolev-Yao model [19], which is a formal (symbolic) model of security of encryptions. In this area, Abadi and Rogaway [1] showed that formally equivalent formulae in the Dolev-Yao model give rise to computationally indistinguishable ciphertexts, if there is no "encryption cycle" (some general types of self-encryption) in the formulae. The authors of [11] studied self-encryption in order to overcome this restriction and formalized the security of self-encryption as *KDM security*, which is a more general notion than the circular security. They also proposed KDM secure encryption w.r.t. all functions based on the random oracle model. Later, Adão, Bana, Herzog, and Scedrov [3] proved formally that the above restriction could be removed if an encryption is KDM secure.

2.3 The Seminal Work of Boneh, Halevi, Hamburg, Ostrovsky and Recent Studies

The most important problem, at the time, was constructing a KDM secure public key encryption without relying on the random oracle idealization. Hofheinz and Unruh [28] partially solved this problem. Later, Boneh, Halevi, Hamburg, and Ostrovsky finally succeeded and proposed the first feasible KDM secure scheme in the standard model in their seminal paper [12]. They achieve KDM secure scheme w.r.t. affine functions, which is quite inefficient.

After this breakthrough, two main lines of research have emerged. The first is the theoretical direction: we want to know the largest function ensembles $\mathcal{F}$ such that there exists a feasible KDM secure scheme w.r.t. $\mathcal{F}$. The second direction considers the more practical side: we want to construct an efficient KDM secure scheme w.r.t. a reasonably large $\mathcal{F}$.

In the first direction, Brakerski, Goldwasser, and Kalai [15] succeeded in proposing an encryption scheme which is KDM secure beyond affine functions. Then later, Barak, Haitner, Hofheinz, and Ishai [8] succeeded in constructing KDM secure scheme w.r.t. all bounded size circuits. On the other hand, an impossibility result of Haitner and Holenstein [25] (which is improved by [8]) showed that there is no black-box construction of KDM secure scheme w.r.t. all (unbounded size) circuits.

In the second direction, constructions that do not encrypt messages bit by bit were considered, but rather do it block-wise. Applebaum, Cash, Peikert, and Sahai [5] proposed an efficient KDM secure scheme w.r.t. affine functions based on lattices. Recently, Malkin, Teranishi, and Yung [30] proposed a KDM secure scheme w.r.t. quite larger function set than the affine function set (i.e. a rational function over Straight Line Programs). The scheme is block-wise and the resulting ciphertext is a function of the function degree and not that of the computational program size.

2.4 Other Works

Next we mention a number of KDM related investigations. Backes, Dürmuth, and Unruh [6] showed that the well-known OAEP encryption is KDM secure. Halevi and Krawczyk [26] generalized the notion of KDM to pseudo-random functions and studied its KDM security. Camenisch, Chandran and Shoup [16] proposed the first KDM and CCA2 secure PKE in the standard model. Green and Hohenberger [23] gave an example of PKE which satisfies the indistinguishability but does not satisfy 2-circular security.

The connection between the adaptive Dolev-Yao model and generalized versions of KDM security were studied by Backes, Pfitzmann, Scedrov [7]. Finally, surprising connections between KDM security and the notions of agility and obfuscation are shown by Acar, Belenkiy, and Bellare, and Cash [2] and Canetti, Kalai, Varia, and Wichs [18], respectively.

3. KDM SECURITY

Next, we define the notion of KDM security, give example of function classes, and discuss a security proof methodology. The reader is assumed to be familiar with basic traditional definitions of public-key encryption schemes and of cryptographic attacks on such systems (i.e., chosen plaintext (CPA) and chosen ciphertext (CCA) attacks).

3.1 Definition

For a public key encryption scheme $\mathcal{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ a security parameter κ, and a natural number n, let

$$(\overrightarrow{\mathrm{pk}}, \overrightarrow{\mathrm{sk}}) \leftarrow \overrightarrow{\mathsf{Kg}}_n(1^\kappa)$$

denote the algorithm which executes Kg n times and outputs the n-tuples of public keys and secret keys. Let pk_i and sk_i denote the i-th element of $\overrightarrow{\mathrm{pk}}$ and $\overrightarrow{\mathrm{sk}}$, respectively.

For the secret key space SkSp and message space MeSp of $\mathcal{PKE}$, let

$$\mathcal{F}^{(n)} \subset \{f \ : \ \mathsf{SkSp}^n \to \mathsf{MeSp}\}, \qquad \mathcal{F} = \cup_{n=1}^{\infty} \mathcal{F}^{(n)}.$$

For $\mathrm{ATK} \in \{\mathrm{CPA}, \mathrm{CCA}\}$, a natural number n, a bit b, and an adversary A, consider the following game:

$$(\overrightarrow{\mathrm{pk}}, \overrightarrow{\mathrm{sk}}) \leftarrow \mathsf{Kg}_n(1^\kappa), \quad b' \leftarrow \mathsf{A}^{\mathcal{O}_{\mathsf{Enc}}^{(b)}, \mathcal{D}_{\mathrm{ATK}}}(\overrightarrow{\mathrm{pk}}), \qquad \text{Output } b'.$$

Above, A is allowed to make polynomial number of queries to oracles:

- If $(i, f) \in [n] \times \mathcal{F}^{(n)}$ is sent to $\mathcal{O}_{\mathsf{Enc}}^{(b)}$, $\mathcal{O}_{\mathsf{Enc}}^{(b)}(i, f)$ answers the following C. Below, 0 be some fixed element of MeSp.

$$C \leftarrow \begin{cases} \mathsf{Enc}(\mathrm{pk}_i, f(\overrightarrow{\mathrm{sk}})) & \text{if } b = 1 \\ \mathsf{Enc}(\mathrm{pk}_i, 0) & \text{Otherwise.} \end{cases}$$

- If $(i, C) \in [n] \times \{0,1\}^*$ is sent to $\mathcal{D}_{\mathrm{ATK}}$, $\mathcal{D}_{\mathrm{CPA}}$ always sends back $\perp$. On the other hand, $\mathcal{D}_{\mathrm{CCA}}$ sends back $\mathsf{Dec}(\mathrm{sk}_i, C)$, as long as C was not an output of $\mathcal{O}_{\mathsf{Enc}}^{(b)}(i, f)$ for some f.

We say that $\mathcal{PKE}$ is $KDM^{(n)}[\mathcal{F}]$-ATK *secure* (or $KDM^{(n)}$-ATK *secure with respect to* $\mathcal{F}$) if the following advantage is negligible for any polynomial time adversary A.

$$\mathsf{Adv.KDM}_{\mathsf{A}}[\mathcal{F}, n] = \left|\Pr[b' = 1 \mid b = 1] - \Pr[b' = 1 \mid b = 0]\right|.$$

We say that $\mathcal{PKE}$ is *KDM*[$\mathcal{F}$]-ATK *secure* if it is $\mathrm{KDM}^{(n)}[\mathcal{F}]$-ATK secure for any n. In this survey, we simply call *KDM security* KDM-CPA security.

The following proposition is simple to verify:

PROPOSITION 1 (**KDM-ATK $\Rightarrow$ IND-ATK**). *KDM*[$\mathcal{F}$]*-ATK security imply indistinguishability against ATK if* $\mathcal{F}$ *contains all constant functions* $\{f_M : \overrightarrow{\mathrm{sk}} \mapsto M\}_M$ *on* MeSp.

3.2 Stronger Definitions

KDM Security for Adaptive Public Key Generations: A stronger definition of KDM security can be considered, where an adversary can get new public keys adaptively by making a query to the challenger.

Some known schemes (e.g. [14]), however, may not satisfy this stronger security notion. This is because they require the maximum n to be fixed before key generation and KDM security is be proved only when n is less than the predetermined maximum.

KDM Security with Corruptions: Backes, Pfitzmann, and Scedrov [7] and Backes, Dürmuth, and Unruh [6] studied stronger variants of KDM security where an adversary can obtain some secret keys adaptively by "corrupting users". This kind of "KDM security with corruption" is required to study Dolev-Yao model, as we will see in Section 5.1.

Defining this notion is not easy because an adversary may get unexpected secret keys other than queried one. E.g. if she knows $\mathsf{Enc}(\mathrm{pk}_1, \mathrm{sk}_2)$, she can get sk_2 also by making reveal query for the secret key sk_1 corresponding to pk_1.

The authors of [7] therefore imposed the following restriction on reveal queries: An adversary can make reveal queries for sk_i only when she has not made encryption query under key pk_i.

However, the authors of [6] then found that the security definition of [7] cannot be used to prove some useful examples of protocols. They therefore gave another definition of "KDM security with corruption" where the restriction on reveal queries is weaker than that of [7], and then they showed that the well-known OAEP encryption scheme [10] satisfies their security notion.

3.3 Examples of KDM function ensembles

Constants. The trivial example of KDM function ensemble $\mathcal{F}$ is the set of all constant functions

$$\{f_M : \overrightarrow{\mathrm{sk}} \mapsto M\}_M$$

on MeSp. KDM security w.r.t. this ensemble is clearly equivalent to indistinguishability (namely semantic security).

Clique and Circular. A simple non trivial example is the set of all selector functions

$$\mathcal{CLQ} = \{P_j : \overrightarrow{\mathrm{sk}} \mapsto \mathrm{sk}_j\}_j.$$

KDM security w.r.t. this ensemble is called *clique security* [12]. This security notion against CPA attacks is clearly equivalent to the following statement:

$\{\mathsf{Enc}(\mathrm{sk}_j, \mathrm{sk}_i)\}_{i,j}$ is indistinguishable from $\{\mathsf{Enc}(\mathrm{sk}_j, 0)\}_{i,j}$.

Circular security has two meanings: the original definition in [17] is equivalent to clique security, but it sometimes refers to a weaker security notion (Strictly Circular Security):

$\{\mathsf{Enc}(\mathrm{sk}_i, \mathrm{sk}_{i+1 \bmod n})\}_i$ is indistinguishable from $\{\mathsf{Enc}(\mathrm{sk}_i, 0)\}_i$.

Projections. *Projection security* [4] refers to KDM security w.r.t.

$$\mathcal{PRJ} = \mathcal{F}_0 \cup \mathcal{F}_1,$$

where

$$\mathcal{F}_0 = \{f_{i,j} : \overrightarrow{\mathrm{sk}} \mapsto (\text{the } j\text{-th bit of } \mathrm{sk}_i)\}_{i,j}$$
$$\mathcal{F}_1 = \{f_{i,j} : \overrightarrow{\mathrm{sk}} \mapsto 1\text{-(the } j\text{-th bit of } \mathrm{sk}_i)\}_{i,j}.$$

Linear and Affine. If the message space is a linear space over $\mathbb{Z}_p$, we can define

$$\mathsf{Lin}(\mathcal{F}) = \{\sum_j a_j f_j \mid a_j \in \mathbb{Z}_p, f_j \in \mathcal{F}\},$$

$$\mathsf{Aff}(\mathcal{F}) = \{c + \sum_j a_j f_j \mid c, a_j \in \mathbb{Z}_p, f_j \in \mathcal{F}\}.$$

for a function ensemble $\mathcal{F}$.

(Bounded Degree) Quotient Straight-Line Program. A function $f(X_1, \ldots, X_n)$ is called *SLP computable* over $\mathbb{Z}_K$ if it can be computed from constants of $\mathbb{Z}_K$ and variables X_k by applying $+$, $-$, and $\cdot$ a polynomial number of times. Clearly, SLP computable function is a polynomial over $\mathbb{Z}_K$ but it may have superpolynomial number of terms[30].

A function f is called *QSLP computable* (stands for Quotient SLP) if we also consider division it satisfies the same definition as above, except division is allowed as well, and we consider a ratio (division) of two SLP computable functions [13]. We require that a QSLP is well-defined in the sense that all denominator of divisions have inverses.

The following ensembles [30] can be defined:

$$\mathcal{SLP}_{\mathsf{poly}}[K] = \{f \mid \deg f \le \mathsf{poly}(\kappa), f \text{ is SLP computable}\}$$
$$\mathcal{QSLP}_{\mathsf{poly}}[K] = \left\{ f \;\middle|\; \begin{array}{l} \deg f \le \mathsf{poly}(\kappa), \\ f \text{ is well-defined QSLP computable} \end{array} \right\}$$

Recall that κ above is the security parameter.

(Bounded) Boolean Circuits [8]. The largest ensemble for which it is feasible to achieve KDM security, is that of bounded Boolean circuits.

$$\mathcal{C}_{\mathsf{poly}} = \left\{ f \;\middle|\; \begin{array}{l} \exists C : \text{circuit with } \mathsf{size}(C) \le \mathsf{poly}(\kappa), \\ f \text{ is computable by } C. \end{array} \right\}$$

3.4 Important Factors

The following factors are important when one constructs a KDM secure scheme:

- The function ensemble $\mathcal{F}$.
- Security: CPA or CCA.
- Idealized random oracle model or not.
- Efficiency.
- Flexibility of parameters.

About efficiency, public key encryption schemes are considered efficient (in some general sense) if they encrypt messages as entire blocks (and not "bit by bit"). Hence, being block-wise encryption or bit-wise encryption scheme is an important factor, for approaching practicality. Many known schemes [12, 16, 8, 15, 14] are bit-wise encryption, although some known schemes are more efficient block-wise ones [5, 30].

"Flexibility of parameters" means whether one can select parameters such as the number of users flexibly. This factor is also an important parameter for assessing efficiency and practicality. In [30] three types of flexibility levels were identified (based on when a parameter is chosen):, "KeyGen bounded," "Enc bounded," and "Unbounded."

"KeyGen bounded" means that one has to fix the maximums of these parameters before the key generation, KDM security holds only when the parameters are less than these maxima, and efficiency of the scheme depends on these maxima.

"Enc bounded" means that we do not have to fix such maxima, and KDM security hold for all values of parameters, but efficiency of the scheme (the size of the ciphertext) depends on the values of parameters (given at encryption time).

"Unbounded" is the same as "Enc bounded" except that efficiency of the scheme is independent of the values of parameters.

3.5 How to Prove KDM Security

Malkin, Teranishi, and Yung [30] gave a general framework for proving KDM security, called *triple mode proof framework*, by abstracting the proof techniques of known schemes [12, 5, 14]. Specifically, a triple mode proof framework is the notion which enables us to overcome the following inherent dilemma.

Dilemma for Proving KDM Security. A simulator in the proof should produce the view of an adversary without knowing the secret keys, because the secrecy of the secret keys should be used in the proof as the intractable problem. However the simulator has to know the secret keys because it has to compute (an encryption of) the value $f(\mathrm{sk}_1, \ldots, \mathrm{sk}_n)$.

Solution. The triple mode proof framework is the mechanism that overcomes the above dilemma by using *two* simulators for the security proof, where the first one knows the secret key but the second one does not.

These two simulators are used to show the indistinguishability of *standard ciphertext*, *faked ciphertext*, *hiding ciphertext*. (See Fig.1.) The standard ciphertext is the same as the ciphertext of the scheme. On the other hand, the *faked ciphertext* can be computed by using query (i, f) of an adversary but without using the secret keys. The *hiding ciphertext* can be computed by using neither a query nor the secret keys.

Since a hiding ciphertext does not depend on the query of an adversary, the indistinguishability of a standard ciphertext and a hiding one clearly implies the KDM security.

4. KNOWN SCHEMES

4.1 Comparisons

Fig.2, taken from [30], shows a comparison among the known schemes in the regular (non idealized) model. Here κ is the security parameter. Note that all schemes except for [16] are KDM-CPA secure, and [16] is KDM-CCA2 secure. Only two schemes [5, 30] are efficient block-wise schemes. Only one scheme [8] provides KDM security against the most general class of all bounded size circuits.

In Fig.2, the "Flexibility of Parameters" category is the one explained in Section 3.4. $\mathcal{F}$ of [5] is the set of functions $f(\overrightarrow{\mathrm{sk}})$ which outputs some blocks of sk. In the row of [8] (resp. [30]) the "size" ℓ represents the number of gates in a circuit (resp. the number of $\{+, -, \cdot, /\}$ in a QSLP) which computes a function $f(\overrightarrow{\mathrm{sk}})$. The value N of [30] is an RSA modulus and s is a constant.

4.2 Scheme in the Random Oracle Model

Schemes in the random oracle (idealized and unrealizable) model are relatively easy due to availability of truly random strings.

Black, Rogaway, and Shrimpton [11] showed that the following simple encryption scheme of Bellare and Rogaway [9] is the KDM-CPA secure with respect to the set of all functions.

$$\mathsf{Enc}(\mathrm{pk}, M) = (\phi_{\mathrm{pk}}(R), \mathcal{H}(R) \oplus M).$$

Above, ϕ_{pk} is a trapdoor one-way permutation, R is a random, and $\mathcal{H}$ is a random oracle. A secret key sk of this scheme is the trapdoor of ϕ_{pk}.

The proof of KDM security is straight forward. The output $\mathcal{H}(R)$ of the random oracle is a truly random string, and therefore hides M perfectly, even if M depends on the secret key. This means that a ciphertext is indistinguishable from random and the KDM security of the scheme therefore holds.

Camenisch and Lysyanskaya [17] also gave another example of KDM secure scheme in the random oracle model which details we omit.

4.3 The [12] scheme w.r.t. Affine Functions

In their seminal work [12] Boneh, Halevi, Hamburg, and Ostrovsky proposed the first KDM secure scheme in the standard model. Let $\mathbb{G}$ be a group of prime order p and g be a fixed generator of $\mathbb{G}$. Their scheme is as follows.

- **Key Generation.** Let $\ell = \lfloor 3 \log_2 p \rfloor$. $g_1, \ldots, g_\ell \xleftarrow{\$} \mathbb{G}$, $s \leftarrow (s_1, \ldots, s_\ell) \xleftarrow{\$} \{0,1\}^\ell$, $h \leftarrow {g_1}^{s_1} \cdots {g_\ell}^{s_\ell}$. Output the following pk and sk:

$$\mathrm{pk} := ((g_j)_{j \in [\ell]}, h), \qquad \mathrm{sk} := (g^{s_j})_{j \in [\ell]}.$$

- **Encryption of $M \in \mathbb{G}$.** Choose $r \xleftarrow{\$} \mathbb{Z}_p$ and output the ciphertext

$$((g_j{}^r)_{j \in [\ell]}, M h^r)$$

- **Decryption of $(c_1, \ldots, c_\ell, d) \in \mathbb{G}^{\ell+1}$.** Compute $(s_1, \ldots, s_\ell)$ from $\mathrm{sk} = (g^{s_1}, \ldots, g^{s_\ell})$. (One can do it in polynomial time because $s_i \in \{0,1\}$.) Output

$$M \leftarrow d \cdot {c_1}^{s_1} \cdots {c_\ell}^{s_\ell}.$$

THEOREM 1 ([12]). *The above scheme is KDM secure with respect to* $\mathsf{Aff}(\mathcal{PRJ})$ *for any* n *under the DDH assumption.*

Dependency of Ciphertexts	sk	(i, f)	
Ciphertext	Yes.	Yes.	} Sim. knows sk.
Faked Ciphertext	No.	Yes.	} Sim. does not know sk.
Hiding Ciphertext	No.	No.	

Figure 1: Triple Mode Simulatable Encryption[30]

	Block -wise?	Functions	|Ciphertext| per |Message|	Flexibility of Parameters			Assum -ption
				# of Users n	max deg d	Size ℓ	
[12] [16]	No.	$\mathsf{Aff}(\mathsf{PRJ})$	$O(\kappa^2)$	Unbounded	-	-	DDH LDDH
[15]		Polynomial of Bits with deg$= O(1)$	$O(\kappa^{d+1})$		KeyGen	-	DDH LWE
[14]		$\mathsf{Aff}(\mathsf{PRJ})$	$O(n\kappa^2 + \kappa^{d+1})$	KeyGen			QR DCR
[8]		Bounded Size Circuit	$O(n\mathsf{poly}(\kappa) + \kappa\ell)$	Enc	-	Enc	DDH LWE
[5]	Yes.	$\mathsf{Aff}(\mathcal{F})$	$O(1)$	Unbounded	-	-	LWE
[30]		$\mathcal{QSLP}_{\mathsf{poly}}[N]$	$O(d)$		Enc	Unbounded	DCR

Figure 2: Comparison of Known Results [30]

Idea Behind the Proof. A starting point of the proof is showing that the ElGamal encryption is KDM secure w.r.t. function $f(s) = (g^a)^s$. Here $a \in \mathbb{Z}_p$ is some constant. We can divert the idea for proving it into the proof of the KDM security of the scheme [12], because the scheme [12] coincides with ElGamal if we let $\ell = 1$, take s_i not from $\{0,1\}^\ell$ but $\mathbb{Z}_p$, and finally set the secret key not to $(g^{s_j})_{j\in[\ell]}$ but to $s = \log_g h$, where (g, h) is a public key.

KDM security of ElGamal w.r.t. $f(s) = (g^a)^s$ is shown as follows. A ciphertext $C = (g^r, Mh^r)$ for a key dependent message $M = (g^a)^s$ can be re-written as follows, by setting $t = r + a$:

$$C = (g^r, (g^a)^s(g^s)^r) = (g^r, g^{s(a+r)}) = (g^{-a}g^t, g^{st}) = (g^{-a}g^t, h^t).$$

The above discussion shows that a ciphertext C is (statistically) indistinguishable from a "faked ciphertext" $(g^{-a}g^t, h^t)$, which is computable from a public key (g, h), the random value t, and a, without using the secret key s!

The DDH assumption implies that (g^t, h^t) is indistinguishable from random pair of group elements. In other words, a faked ciphertext $(g^{-a}g^t, h^t)$ is indistinguishable from a "hiding ciphertext" (random,random).

The above discussion shows that a ciphertext C is indistinguishable from a the hiding ciphertext, which is independent from the function $f(s) = (g^a)^s$ queried by an adversary. This means that the KDM security holds.

We can prove KDM security of [12] based on the above idea, although it is much harder involving linear algebra arguments.

4.4 A Lattice based Scheme

Applebaum et.al. [5] constructed a KDM secure scheme using the Learning With Errors (LWE) assumption [35], which is a lattice based assumption. Their public key and an encryption of a message M is as follows:

$$\mathrm{pk} = (A, B), \qquad C = (Ar, Br + Mp + e) \bmod p^2,$$

where p is a prime, A and B are some matrix over $\mathbb{Z}_{p^2}$, r is a random value, and e is some randomly selected "error".

Their scheme is similar to ElGamal encryption in some sense: In fact, if we remove e and p, a ciphertext becomes

$$C = (Ar, Br + M),$$

which is an "additive version" of ElGamal. The KDM security of ElGamal was given above in Section 4.3, and the security proof of the current scheme indeed resembles that proof.

4.5 Scheme w.r.t. Bounded Boolean Circuits

Barak, Haitner, Hofheinz, and Ishai [8] constructed a KDM secure scheme w.r.t. the set of bounded Boolean circuits.

The starting point of their scheme is fully homomorphic encryption [20]. A *fully homomorphic encryption* is an encryption scheme such that $\mathsf{Enc}(\mathrm{pk}, f(M))$ can be computed from $\mathsf{Enc}(\mathrm{pk}, M)$ for any polynomial size circuit f.

If a fully homomorphic encryption also satisfies the property $\mathsf{Enc}(\mathrm{pk}, \mathrm{sk}) \simeq \mathsf{Enc}(\mathrm{pk}, \mathrm{random})$, it is immediately KDM secure for all functions because the fully homomorphic property, the above property, and the semantic security of Enc imply $\mathsf{Enc}(\mathrm{pk}, f(\mathrm{sk})) \simeq \mathsf{Enc}(\mathrm{pk}, f(\mathrm{random})) \simeq \mathsf{Enc}(\mathrm{pk}, 0)$.

However, there is no known scheme that satisfies all of the above properties. The authors of [8] therefore replace the fully homomorphic encryption of the above scheme with Yao's garbled circuits. Informally, a *garbled circuit* $\mathsf{GC}(h, K)$ is a polynomial time computable function which takes a bounded Boolean circuit h and a "key" $K = (K_{i,j})_{i\in\{0,1\},j\in[m]}$. For a bit string $x = x_1||\cdots||x_m$, let K_x be $(K_{x_j,j})_{i\in\{0,1\},j\in[m]}$. Then the garbled circuit satisfies the following properties:

- If one knows K_x, one can compute the value $h(x)$ from $\mathsf{GC}(h, K)$.
- Even if one knows K_x, $\mathsf{GC}(h, K)$ and $\mathsf{GC}(h', K)$ are indistinguishable for every h and h' satisfying $h(x) = h'(x)$.

- If one does not know K, $\mathsf{GC}(h, K)$ and $\mathsf{GC}(h', K)$ are indistinguishable for every h and h'.

A public key pk and an encryption $C = \mathsf{Enc}(\mathrm{pk}, M)$ of a message M in [8] are as follows. Bellow, $\mathsf{TEnc}^{(i,j)}$ is an encryption satisfying some special property which we will explain later, $\mathrm{pk}_{i,j}$ is a public key for $\mathsf{TEnc}^{(i,j)}$, and h_M is a circuit which always outputs M.

$$\mathrm{pk} = (\mathrm{pk}_{i,j})_{i,j}$$

$$\mathsf{Enc}(\mathrm{pk}, M) = ((\mathsf{TEnc}^{(i,j)}(\mathrm{pk}_{i,j}, K_{i,j}))_{i,j}, \mathsf{GC}(h_M, K)).$$

To decrypt the above ciphertext, K is recovered from the first part of the ciphertext using the secret keys, and then $h_M(0)$ is computed from $\mathsf{GC}(h_M, K)$ and K. Since h_M always outputs M, the recovered message $h_M(0)$ is equal to M.

$\mathsf{Enc}^{(i,j)}$ is an encryption function of a *target encryption scheme* [8]. Informally, a target encryption scheme $(\mathsf{TKg}, (\mathsf{TEnc}^{(i,j)})_{i,j}, \mathsf{TDec})$ is a tuple of polynomial time algorithms satisfying the following properties, where $(\mathrm{pk}, \mathrm{sk})$ is a key pair generated by $\mathsf{TKg}(1^\kappa)$, sk_i is the i-th bit of sk, and $\overline{\mathrm{sk}}_i$ is $1 - \mathrm{sk}_i$.

- $\mathsf{TDec}(\mathrm{sk}, \mathsf{TEnc}^{(i,\mathrm{sk}_i)}(\mathrm{pk}, M)) = M$ holds for any M and i.
- $\mathsf{TEnc}^{(i,\overline{\mathrm{sk}}_i)}(\mathrm{pk}, M)$ and $\mathsf{TEnc}^{(i,\overline{\mathrm{sk}}_i)}(\mathrm{pk}, M')$ have statistically indistinguishable distributions for any M, M' and i.
- $(\mathrm{pk}, \mathsf{TEnc}^{(i,j)}(\mathrm{pk}, M))$ and $(\mathrm{pk}, \mathsf{TEnc}^{(i,j)}(\mathrm{pk}, M'))$ have computationally indistinguishable distributions for any M, M' and i.

The authors of [8] showed that target encryptions can be constructed based on DDH and LWE assumptions. Hence KDM secure scheme w.r.t. bounded size circuits can be constructed based on a DDH or LWE assumption (and the existence of garbled circuits). We note that, obviously, the resulting ciphertext in the scheme is a very large function of the circuit size.

4.6 CCA and KDM secure scheme

Camenisch, Chandran, and Shoup [16] gave a general method to construct KDM-CCA secure scheme based on Naor-Yung dual encryption technique [33]. Specifically, they construct their scheme based on a KDM[$\mathcal{F}$]-CPA secure encryption $\Pi_{\mathsf{KDM}} = (\mathsf{Kg}_{\mathsf{KDM}}, \mathsf{Enc}_{\mathsf{KDM}}, \mathsf{Dec}_{\mathsf{KDM}})$, IND-CCA2 secure encryption $\Pi_{\mathsf{CCA}} = (\mathsf{Kg}_{\mathsf{CCA}}, \mathsf{Enc}_{\mathsf{CCA}}, \mathsf{Dec}_{\mathsf{CCA}})$, and a NIZK (Non-Interactive Zero-knowledge Proof). The details of their scheme are as follows.

- **Key Generation.** Generate key pairs $(\mathrm{pk}_1, \mathrm{sk}_1)$ and $(\mathrm{pk}_2, \mathrm{sk}_2)$ of Π_{KDM} and Π_{CCA}. Generate a CRS σ for NIZK. Output $\mathsf{PK} = (\mathrm{pk}_1, \mathrm{pk}_2, \sigma)$ and $\mathsf{SK} = \mathrm{sk}_1$.
- **Encryption of M.** Compute and output the following C.

  $$C = (\mathsf{Enc}_{\mathsf{KDM}}(\mathrm{pk}, M), \mathsf{Enc}_{\mathsf{CCA}}(\mathrm{pk}, M), \mathsf{pf}).$$

  Here pf is a NIZK which proves that the first two components of C encrypt the same messages.
- **Decryption of C.** Parse C as (C_1, C_2, pf). If pf is invalid, output $\perp$. Otherwise, recover message from C_1 using SK.

The KDM[$\mathcal{F}$] security and the CCA security of C follows from those of $\mathsf{Enc}_{\mathsf{KDM}}(\mathrm{pk}, M)$ and $\mathsf{Enc}_{\mathsf{CCA}}(\mathrm{pk}, M)$. The scheme of [16] is therefore KDM[$\mathcal{F}$]-CCA secure.

Camenisch et.al. [16] also gave the concrete scheme, more secure than the generic one, where Π_{KDM} is (a LDDH based variant of) [12], Π_{CCA} is [38, 27], and NIZK is Groth-Sahai proof system [24].

4.7 KDM$^{(1)}$ Secure Scheme w.r.t. $\mathsf{Lin}((\phi_j)_{j\in[m]})$

Brakerski, Goldwasser, and Kalai [15] proposed a KDM$^{(1)}$ secure scheme w.r.t. $\mathsf{Lin}((\phi_j)_{j\in[m]})$, where $\phi_1, \ldots, \phi_m$ are polynomial time computable functions $\mathsf{SkSp} \to \mathsf{MeSp}$ *fixed in advances*. (Here KDM$^{(1)}$ security means that KDM security for a single key. See Section 3.1 for the definition of this.)

Their scheme is constructed by modifying the scheme of [12]: Their key generation selects secret key $\mathrm{sk} \leftarrow s \leftarrow (s_1, \ldots, s_k) \xleftarrow{\$} \{0,1\}^k$ randomly and sets

$$s_{k+i} \leftarrow \phi_i(s_1, \ldots, s_k), \text{ for } i \in [m], \quad \bar{s} \leftarrow (s_1, \ldots, s_\ell),$$

where k is some parameter and $\ell = k + m$. The other parts of the scheme are the same as those of [12] except that one uses $\bar{s}$ instead of s when generating pk and decrypting a ciphertext.

Specifically, their scheme is as follows (bellow, k and m are parameters).

- **Key Generation.** Let $\ell \leftarrow k + m$. $g_1, \ldots, g_\ell \xleftarrow{\$} \mathbb{G}$, $s \leftarrow (s_1, \ldots, s_k) \xleftarrow{\$} \{0,1\}^k$, $s_{k+i} \leftarrow \phi_i(s_1, \ldots, s_k)$ for $i \in [m]$, $h \leftarrow {g_1}^{s_1} \cdots {g_\ell}^{s_\ell}$. Output the following pk and sk:

  $$\mathrm{pk} := ((g_j)_{j\in[\ell]}, h), \qquad \mathrm{sk} := (g^{s_j})_{j\in[\ell]}.$$

- **Encryption of $M \in \mathbb{G}$.** Choose $r \xleftarrow{\$} \mathbb{Z}_p$ and output the ciphertext

  $$((g_j{}^r)_{j\in[\ell]}, M h^r)$$

- **Decryption of $(c_1, \ldots, c_\ell, d) \in \mathbb{G}^{\ell+1}$.** Compute $(s_1, \ldots, s_\ell)$ from $\mathrm{sk} = (g^{s_1}, \ldots, g^{s_\ell})$. (One can do it in polynomial time because $s_i \in \{0,1\}$.) Output

  $$M \leftarrow d \cdot {c_1}^{s_1} \cdots {c_\ell}^{s_\ell}.$$

For suitable choice of k, their scheme become KDM secure under the DDH assumption.

They also showed that their scheme became KDM secure w.r.t. the set of polynomials of bits of secret keys with degree $\leq d$, by setting $\phi_i = {s_1}^{\varepsilon_1} \cdots {s_k}^{\varepsilon_k}$ for $i = \varepsilon_1 || \cdots || \varepsilon_k$ and $\varepsilon_1 + \cdots + \varepsilon_k \leq d$.

They also gave a sufficient condition characterizing when their technique is applicable to a scheme, and use it to apply their technique to the scheme of [5], resulting in a scheme based on the LWE assumption.

4.8 KDM Secure Schemes w.r.t. Affine Functions based on QR and DCR Assumptions.

Brakerski and Goldwasser [14] proposed a general framework of assumptions (implying the QR and the DCR assumptions as special cases) and proposed a KDM secure scheme w.r.t. the set $\mathsf{Aff}(\mathcal{PRJ})$ of affine functions based on assumptions contained in this framework.

Their scheme itself is similar to that of [12], that is

$$\mathrm{sk} = (s_1, \ldots, s_\ell), \quad \mathrm{pk} = ((g_j)_{j\in[\ell]}, h), \quad \text{where } h = {g_1}^{s_1} \cdots {g_\ell}^{s_\ell}$$

$$\mathsf{Enc}_{\mathrm{pk}}(M) = ((g_j{}^r)_{j\in[\ell]}, T^M h^r) \bmod N,$$

where $M \in \{0,1\}$ is a message, and T is -1 or $1+N$ if the assumption is QR or DCR, respectively. They also showed that their scheme is leakage resilient and auxiliary input resilient.

The security proof of their scheme, in turn, is based on a new proof technique. If we use the term of triple mode proof framework of [30], their proof technique can be described as follows: they prove the computational indistinguishability of the ciphertext of the message $M = b + \sum_j a_j s_j$ and a "faked ciphertext" $((T^{a_j} g_j{}^r)_{j\in[\ell]}, T^b h^r)$ based on the secrecy of the random value r.

4.9 Scheme w.r.t. Bounded Degree SLP and QSLP

The scheme of Malkin, Teranishi, and Yung [30], called *d-Cascaded Paillier ElGamal*, is computed recursively as follows: Let N be an RSA modulus and $s \geq 2$ be a natural number. First, a "Paillier ElGamal" encryption $(e_0, c_0) = ({u_0}^{-1}, T^M v_0) \mod N^s$ of a message M is computed, where $T = 1+N$ and $(u_0, v_0) \leftarrow (g^{r_0}, h^{r_0})$. Next, the left component e_i of the ciphertext is encrypted by "Paillier ElGamal" encryption and $(e_{i+1}, c_{i+1}) = ({u_{i+1}}^{-1}, e_i v_{i+1})$ is obtained for $i = 1, \ldots, d-1$, where $(u_{i+1}, v_{i+1}) \leftarrow (g^{r_{i+1}}, h^{r_{i+1}})$. We finally let c_{d+1} be e_d.

The d-cascaded Paillier ElGamal encryption of message M is the tuple

$$\begin{aligned} C &= (c_{d+1}, c_d, c_{d-1}, \ldots, c_0) \\ &= ({u_d}^{-1}, {u_{d-1}}^{-1} v_d, {u_{d-2}}^{-1} v_{d-1}, \ldots, T^M v_0) \bmod N^s. \end{aligned}$$

The details of the scheme are as follows: Bellow, we assume that N which is a product of two safe primes and $g \in \{u^{2N} \bmod N^s \mid u \in \mathbb{Z}_N\}$ are public. We will let T denote $1+N$.

- $\mathsf{Kg}(prm)$: Select $\mathrm{sk} \leftarrow x \xleftarrow{\$} [2^\xi \cdot \lfloor N/4 \rfloor]$ randomly, compute $\mathrm{pk} \leftarrow h \leftarrow g^x \bmod N^s$, and output $(\mathrm{pk}, \mathrm{sk})$.
- $\mathsf{Enc}_{prm}(\mathrm{pk}, M)$ for $M \in \mathbb{Z}_{N^{s-1}}$: Select $r_0, \ldots, r_d \xleftarrow{\$} [\lfloor N/4 \rfloor]$ randomly, compute the following $c_0, \ldots, c_{d+1}$ and output $C \leftarrow (c_{d+1}, \ldots, c_0)$.

$$c_j \leftarrow \begin{cases} T^M h^{r_0} & \bmod N^s \quad \text{if } j = 0 \\ g^{-r_{j-1}} h^{r_j} & \bmod N^s \quad \text{if } j \in \{1, \ldots, d\} \\ g^{-r_d} & \bmod N^s \quad \text{if } j = d+1. \end{cases}$$

- $\mathsf{Dec}_{prm}(\mathrm{sk}, C)$: Parse C as $(c_{d+1}, \ldots, c_0)$ and compute and output the following M:

$$M \leftarrow L(c_0 {c_1}^x \cdots {c_{d+1}}^{x^{d+1}} \bmod N^s).$$

where L is the function such that for all $M \in \mathbb{Z}_{N^{s-1}}$, $L(T^M) = M \bmod N^{s-1}$.

Their scheme is KDM secure w.r.t. SLP (i.e., straight line program) computable polynomial f with degree $\leq d$ modulo N^s. The idea behind the proof is as follows: Let $f(x)$ be a polynomial with degree d (which is a special case of a SLP computable function). Based on the technique of [14], they showed that $(g^{-r}, T^{f(x)} h^r)$ is indistinguishable from $(T^{f'(x)} g^{-r}, T^b h^r)$, where $f(s) = f'(s)s + b$. Now the right term is independent of the secret key, and the left term does depend on the secret key, but only as a degree $d-1$ polynomial $f'(x)$. Hence, recursive encryption of [30] enables us to reduce the degree to 1.

The authors of [30] also gave a KDM secure scheme w.r.t. QSLP which is a quotient of SLP's computable polynomial f with degree $\leq d$ modulo N. Intuitively, the scheme has two ciphertexts where the first and the second ciphertexts correspond to the numerator and the denominator of the Quotient SLP, respectively (which are encryptions of non-zero representing SLP's).

5. APPLICATIONS

5.1 Dolev-Yao Model

The *Dolev-Yao model*[19] is the security model of an "ideal world" which is defined by a formal symbolic logic. Intuitively, this model treats an ideal encryption $\{M\}_K$ of a bit string M, wher one can decrypt it only if he "knows" the key K.

In this model words of bit strings, keys and encryptions, such as $K_1||\{M||\{K_1\}_{K_2}\}_{K_1}$, are considered. Each word called *expression* can be simplified by decryption. E.g. the above expression can be simplified by obtaining K_1 from it and decrypting $\{M||\{K_1\}_{K_2}\}_{K_1}$ by K_1. The process of the simplification is called *entailment*. Two expressions are called *equivalent* if their entailed forms have essentially the same pattern.

The Dolev-Yao model is related to KDM security because "self-encryption," e.g., $\{K\}_K$ can be symbolically described in this model.

The result of Abadi and Rogaway [1] (improved by [11, 3, 7]) shows the following facts:

THEOREM 2. *(Soundness Theorem, informal) Let* $\Pi = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ *be a public key encryption scheme which is KDM secure w.r.t. any functions. Then, if two expressions* X *and* Y *are equivalent,* $[|X|]_\Pi$ *and* $[|Y|]_\Pi$ *are indistinguishable. Here* $[|X|]_\Pi$ *is a bit-string which is obtained by replacing* $\{\cdot\}$. *in* X *with* $\mathsf{Enc}(\cdot,\cdot)$.

Backes, Pfitzmann, and Scedrov [7] generalized the above soundness theorem to the case of active attacks. Specifically, they formalized a notion "KDM security with corruption" called this notion DKEM security, and showed that the soundness theorem of (BRSIM)/UC [34] holds under DKEM security.

5.2 Fully Homomorphic Encryption

Recall that a *fully homomorphic encryption* is an encryption scheme such that $\mathsf{Enc}(\mathrm{pk}, f(M))$ can be computed from $\mathsf{Enc}(\mathrm{pk}, M)$ for any polynomial size circuit f.

In a seminal work [20], Gentry succeeded in proposing a *leveled* fully homomorphic encryption scheme. His scheme uses as a component a leveled scheme, leveled in the sense that the encryption algorithm Enc depends on a parameter d and a homomorphic operation can be applied to a ciphertext only when the size of f is smaller than d (and the ciphertext is computed using d). Specifically, $\mathsf{Enc}^{(0)}(f(M))$ can be computed from f with size $\leq d$ and $\mathsf{Enc}^{(d)}(M)$. That is,

$$(f, \mathsf{Enc}^{(d)}(\mathrm{pk}, M)) \mapsto \mathsf{Enc}^{(0)}(\mathrm{pk}, f(M)).$$

The scheme is constructed as follows. First, an encryption scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$ is constructed such that $\mathsf{Enc}'(\mathrm{pk}_{i+1},$

$f(M)$) can be computed from f whose size is bounded by small constant, $\mathsf{Enc}'(\mathrm{pk}_i, M)$ and $\mathsf{Enc}'(\mathrm{pk}_{i+1}, \mathrm{sk}_i)$. That is,

$$(f, \mathsf{Enc}'(\mathrm{pk}_i, M), \mathsf{Enc}'(\mathrm{pk}_{i+1}, \mathrm{sk}_i)) \mapsto \mathsf{Enc}'(\mathrm{pk}_{i+1}, f(M)). \quad (1)$$

Here i is an integer and $(\mathrm{pk}_i, \mathrm{sk}_i)$ and $(\mathrm{pk}_{i+1}, \mathrm{sk}_{i+1})$ are key pairs generated by $\mathsf{Kg}'(1^\kappa)$.

Second, the public key pk of the scheme is allowed to be $(\mathrm{pk}_i, \mathsf{Enc}(\mathrm{pk}_i, \mathrm{sk}_{i-1}))_{i\in[d]}$, where $(\mathrm{pk}_i, \mathrm{sk}_i)$ is a key pair generated by $\mathsf{Kg}'(1^\kappa)$. Gentry then let

$$\mathsf{Enc}^{(d)}(\mathrm{pk}, M) := \mathsf{Enc}'(\mathrm{pk}_d, M).$$

The leveled fully homomorphic property of his scheme can be achieved by applying equation (1) above d times.

Gentry then points out that KDM security can be used to achieve the full non-leveled construction of a fully homomorphic encryption: Indeed, the above scheme achieves non-leveled fully homomorphic property if it holds that $(\mathrm{pk}_i, \mathrm{sk}_i) = (\mathrm{pk}_{i+1}, \mathrm{sk}_{i+1})$. The KDM security ensures the secrecy of sk_i in a ciphertext $\mathsf{Enc}'(\mathrm{pk}_{i+1}, \mathrm{sk}_i)$ even if $(\mathrm{pk}_i, \mathrm{sk}_i) = (\mathrm{pk}_{i+1}, \mathrm{sk}_{i+1})$.

5.3 Anonymous Credential System

An *Anonymous Credential System* is a system in which a user can obtain a credential from organizations and can prove the possession of these credentials anonymously.

Specifically, each user has k keys pairs $(\mathrm{pk}_i, \mathrm{sk}_i)$ (or "credentials") representing notions like a driver licence or a passport, and can prove the possession of credentials by executing zero-knowledge proofs.

To discourage delegation of credentials, we make the user publish "circular" encryption

$$\mathsf{Enc}(\mathrm{pk}_1, \mathrm{sk}_2), \mathsf{Enc}(\mathrm{pk}_2, \mathrm{sk}_3), \ldots, \mathsf{Enc}(\mathrm{pk}_n, \mathrm{sk}_1).$$

Then the user is in an "all-or-nothing" situation where he has to reveal all secret keys if he wants to delegate only one of them! For the above publication the encryption scheme Enc should be KDM secure.

5.4 Relationship with Agility

We call a function ensemble $\mathcal{E}$ *k-agile* w.r.t. weak PRF (Pseudo Random Function) if any adaptively selected k-element $F_1, \ldots, F_k$ of $\mathcal{E}$ is weak PRF even if the components use the same key K. Here a polynomial time computable deterministic function F is called *weak PRF* if $(F(x_1), F(x_2), \cdots)$ is indistinguishable from random when $x_1, x_2, \ldots$ are selected randomly.

Acar, Belenkiy, Bellare, and Cash [2] showed by using KDM security that the set of all weak PRF is not k-agile for any $k \geq 2$ (or this set is empty).

This fact was proved by contradiction as follows. From the assumption, there exists weak PRF f. For a public key (or secret key) encryption scheme $\Pi = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$, key $\bar{K} = (L, K_1, K_2)$, and an input x, let

$$F^{(1)}_{\bar{K}}(x) := \mathsf{Enc}(K_1, K_2; f_L(x))$$
$$F^{(2)}_{\bar{K}}(x) := \mathsf{Enc}(K_2, K_1; f_L(x)).$$

Then they showed that, if $\{F^{(1)}, F^{(2)}\}$ are 2-agile, assuming IND-R ("Indistinguishable from random") security for Π implies the following property (2-circularity):

$$(\mathsf{Enc}(K_1, K_2), \mathsf{Enc}(K_2, K_1)) \simeq (\mathrm{Rand}_1, \mathrm{Rand}_2)$$

They finally showed that there existed an encryption scheme which was IND-R but is not 2-circular. Hence the set of all weak PRF is not k-agile for any $k \geq 2$ (or this set is empty).

5.5 Relationship with Point Obfuscation

An algorithm O is called (multi-bit) *point obfuscator* if it satisfies the following two properties:

- One can compute M easily from $O(K, M)$ and "key" K.
- One cannot compute M from $O(K, M)$ if she does not know K.

Canetti, Kalai, Varia, and Wichs [18] showed that O was point obfuscator iff the following symmetric key encryption scheme was CPA secure for weak key K:

$$\mathsf{Enc}(K, M) = O(K, M)$$

They also showed that the above theorem hold even if M was related to K, when we replace "CPA" with "KDM".

6. OTHER WORKS

6.1 Impossibility Results

Haitner and Holenstein [25] showed an impossibility results about KDM security. To this end they defined two notions whose intuitive meanings are as following.

- A *cryptographic game* is a polynomial time algorithm which takes a security parameter as an input, interacts with a polynomial time adversary, and outputs 1 or 0. An example of a cryptographic game is the game of DDH.
- A *strongly black-box reduction* from KDM security w.r.t. $\mathcal{F}$ to a cryptographic game is a polynomial time reduction which uses an adversary for KDM security *and queries of the adversary* as black-boxes.

The first impossibility result of Haitner and Holenstein [25] is:

THEOREM 3. *(informal) There exists no strongly black-box reduction from KDM security of a public key encryption w.r.t. all functions to* any *cryptographic game.*

Note that the above result is strengthened by [8].

The second impossibility result of [25] is formalized using the following notion [36]:

- A *fully black-box reduction* from KDM security w.r.t. $\mathcal{F}$ to a one way permutation that consists of the following two algorithms:
  - A polynomial time algorithm which takes a description of a one way permutation f and outputs a description of a public key encryption Π^f.
  - A polynomial time reduction from KDM security of Π^f w.r.t. $\mathcal{F}$ to one way permutation f such that the reduction uses f and an adversary for KDM security as black-boxes.

THEOREM 4. *(informal) There exists no fully black-box reduction from KDM security w.r.t. all functions to a one way permutation.*

6.2 CPA Does Not Imply KDM

Known CPA secure scheme may remain secure even if one encrypts secret keys. A natural question [12] is whether CPA security implies KDM security. Green and Hohenberger [23] gave a counter example to this. Specifically, they gave an example of a CPA secure public key encryption such that one can recover secret keys when given 2-circular encryption $(\mathsf{Enc}(\mathrm{pk}_1, \mathrm{sk}_2), \mathsf{Enc}(\mathrm{pk}_2, \mathrm{sk}_1))$. Note that Acar, Belenkiy, Bellare, and Cash [2] also gave another counter example independently. The authors of [23] also gave a counter example for the case of CCA secure scheme.

6.3 KDM Security of Other Primitives

KDM security of primitives other than public key encryption were studied, considering symmetric key encryptions and PRFs, where KDM security is called *KDI security* [26] (stand for Key Dependent Input).

KDI Security for PRFs. KDI Security for PRFs is defined [26] as following: Let $\{F_K : X \to Y\}$ be a family of PRFs, $\mathcal{K}$ be a key space of F, and $\mathcal{F}$ be a ensemble of functions from $\mathcal{K}$ to X. For a bit b, a security parameter κ, consider the following game:

$$K \leftarrow (\text{rand.}), \quad b' \leftarrow \mathsf{A}^{\mathcal{O}_K^{(b)}, \mathcal{O}_K'^{(b)}}(1^\kappa), \quad \text{Output } b'.$$

Here $\mathcal{O}_K^{(b)}$ and $\mathcal{O}_K'^{(b)}$ are the following oracles:

- $\mathcal{O}_K^{(0)}(\cdot)$ is $F_K(\cdot)$ and $\mathcal{O}_K^{(1)}(\cdot)$ is a random oracle from X to Y.
- On inputting a function $f \in \mathcal{F}$, $\mathcal{O}_K'^{(b)}$ returns $\mathcal{O}_K^{(b)}(f(K))$.

We say that PRF F_K is *KDI secure w.r.t.* $\mathcal{F}$ if the following advantage is negligible for any polynomial time adversary A:

$$\mathsf{Adv.KDM}_{\mathsf{A}}[\mathcal{F}] = \left|\Pr[b' = 1 \mid b = 1] - \Pr[b' = 1 \mid b = 0]\right|.$$

The aspects of KDI security of PRFs is quite different from that of KDM security of public key encryptions, because of the determinism of PRFs. For instance, it is impossible to construct KDI secure PRFs w.r.t. all function because of the following reason[26]:

Let g_i and g_i' be functions such that $g_i(K) = g_i'(K)$ holds iff the i-th bit of K is 0. Then an adversary A can know the i-th bit of the secret key K by making query g_i and g_i' to the oracle $\mathcal{O}'^{(b)}$ (if $b = 0$). Hence, A can gets the secret key K and can distinguish whether $b = 0$ or not by using K.

KDM Security for Symmetric Key Encryptions. KDM security [11, 5] for symmetric key encryptions is defined in the same way as the definition of KDM security for public key encryptions. We therefore omit the details.

KDM security for symmetric key encryptions was first studied by Black, Rogaway, and Shrimpton [11] . They showed that the following scheme $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ is KDM-CPA secure w.r.t. all functions in the random oracle model. Bellow $\mathcal{H}$ is a random oracle and κ is a security parameter.

- $\mathsf{Kg}(1^\kappa)$: Choose $K \xleftarrow{\$} \{0,1\}^\kappa$ and output K.
- $\mathsf{Enc}(K, M)$: Choose $R \xleftarrow{\$} \{0,1\}^\kappa$ and output
$$C \leftarrow (R, \mathcal{H}(K||R) \oplus M)$$
- $\mathsf{Dec}(K, C)$: Parse C as (R, C'). Compute and output
$$M \leftarrow \mathcal{H}(K||R) \oplus C'.$$

Later, Halevi and Krawczyk [26] succeeded in constructing KDM secure scheme w.r.t. a single function in the standard model based on PRF, (although their definition of security is different from ours.)

Then Applebaum, Cash, Peikert, and Sahai [5] proposed a KDM secure scheme w.r.t. affine sum of blocks of the secret key. Their scheme is constructed based on similar idea to their public key encryption scheme and the security of their scheme is proved under the LPN assumption (stand for Leaning Parity with Noise) [35].

7. REFERENCES

[1] M. Abadi and P. Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *J. Cryptology*, 20(3):395, 2007.

[2] T. Acar, M. Belenkiy, M. Bellare, and D. Cash. Cryptographic agility and its relation to circular encryption. In Gilbert [21], pages 403–422.

[3] P. Adão, G. Bana, J. Herzog, and A. Scedrov. Soundness of formal encryption in the presence of key-cycles. In S. D. C. di Vimercati, P. F. Syverson, and D. Gollmann, editors, *ESORICS*, volume 3679 of *Lecture Notes in Computer Science*, pages 374–396. Springer, 2005.

[4] B. Applebaum. Key-dependent message security: Generic amplification and completeness theorems. Cryptology ePrint Archive, Report 2010/513, 2010. http://eprint.iacr.org/.

[5] B. Applebaum, D. Cash, C. Peikert, and A. Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In S. Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 595–618. Springer, 2009.

[6] M. Backes, M. Dürmuth, and D. Unruh. Oaep is secure under key-dependent messages. In J. Pieprzyk, editor, *ASIACRYPT*, volume 5350 of *Lecture Notes in Computer Science*, pages 506–523. Springer, 2008.

[7] M. Backes, B. Pfitzmann, and A. Scedrov. Key-dependent message security under active attacks - BRSIM/UC-soundness of Dolev-Yao-style encryption with key cycles. *Journal of Computer Security*, 16(5):497–530, 2008.

[8] B. Barak, I. Haitner, D. Hofheinz, and Y. Ishai. Bounded key-dependent message security. In Gilbert [21], pages 423–444.

[9] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM Conference on Computer and Communications Security*, pages 62–73, 1993.

[10] M. Bellare and P. Rogaway. Optimal asymmetric encryption. In *EUROCRYPT*, pages 92–111, 1994.

[11] J. Black, P. Rogaway, and T. Shrimpton. Encryption-scheme security in the presence of key-dependent messages. In K. Nyberg and H. M. Heys, editors, *Selected Areas in Cryptography*, volume 2595 of *Lecture Notes in Computer Science*, pages 62–75. Springer, 2002.

[12] D. Boneh, S. Halevi, M. Hamburg, and R. Ostrovsky. Circular-secure encryption from decision Diffie-Hellman. In D. Wagner, editor, *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 108–125. Springer, 2008.

[13] D. Boneh and R. Venkatesan. Breaking RSA may not be equivalent to factoring. In *EUROCRYPT*, pages 59–71, 1998.

[14] Z. Brakerski and S. Goldwasser. Circular and leakage resilient public-key encryption under subgroup indistinguishability - (or: Quadratic residuosity strikes back). In T. Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2010.

[15] Z. Brakerski, S. Goldwasser, and Y. Kalai. Circular-secure encryption beyond affine functions. Cryptology ePrint Archive, Report 2009/485, 2009. http://eprint.iacr.org/ to appear in TCC 2010.

[16] J. Camenisch, N. Chandran, and V. Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In A. Joux, editor, *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 351–368. Springer, 2009.

[17] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In B. Pfitzmann, editor, *EUROCRYPT*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer, 2001.

[18] R. Canetti, Y. T. Kalai, M. Varia, and D. Wichs. On symmetric encryption and point obfuscation. In D. Micciancio, editor, *TCC*, volume 5978 of *Lecture Notes in Computer Science*, pages 52–71. Springer, 2010.

[19] D. Dolev and A. C.-C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–207, 1983.

[20] C. Gentry. Fully homomorphic encryption using ideal lattices. In M. Mitzenmacher, editor, *STOC*, pages 169–178. ACM, 2009.

[21] H. Gilbert, editor. *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*. Springer, 2010.

[22] S. Goldwasser and S. Micali. Probabilistic encryption. *J. Comput. Syst. Sci.*, 28(2):270–299, 1984.

[23] M. Green and S. Hohenberger. CPA and CCA-secure encryption systems that are not 2-circular secure. Cryptology ePrint Archive, Report 2010/144, 2010. http://eprint.iacr.org/.

[24] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In Smart [39], pages 415–432.

[25] I. Haitner and T. Holenstein. On the (im)possibility of key dependent encryption. In O. Reingold, editor, *TCC*, volume 5444 of *Lecture Notes in Computer Science*, pages 202–219. Springer, 2009.

[26] S. Halevi and H. Krawczyk. Security under key-dependent inputs. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, *ACM Conference on Computer and Communications Security*, pages 466–475. ACM, 2007.

[27] D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. In A. Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 553–571. Springer, 2007.

[28] D. Hofheinz and D. Unruh. Towards key-dependent message security in the standard model. In Smart [39], pages 108–126.

[29] M. Liskov, R. L. Rivest, and D. Wagner. Tweakable block ciphers. In M. Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2002.

[30] T. Malkin, I. Teranishi, and M. Yung. Efficient block-wise PKE with KDM security under a flexible slp queries. Cryptology ePrint Archive, 2011. http://eprint.iacr.org/ (to appear).

[31] IEEE P1619. Standard for cryptographic protection of data on block-oriented storage devices, 2007.

[32] IEEE P1619 email archive, 2007. http://grouper.ieee.org/groups/1619/email.

[33] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *STOC*, pages 427–437. ACM, 1990.

[34] B. Pfitzmann and M. Waidner. Composition and integrity preservation of secure reactive systems. In *ACM Conference on Computer and Communications Security*, pages 245–254, 2000.

[35] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009.

[36] O. Reingold, L. Trevisan, and S. P. Vadhan. Notions of reducibility between cryptographic primitives. In M. Naor, editor, *TCC*, volume 2951 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2004.

[37] P. Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes ocb and pmac. In P. J. Lee, editor, *ASIACRYPT*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004.

[38] H. Shacham. A Cramer-Shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive, Report 2007/074, 2007. http://eprint.iacr.org/.

[39] N. P. Smart, editor. *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*. Springer, 2008.