論文 / 著書情報
Article / Book Information

題目(和文)	実用的な属性ベース暗号と属性ベース署名に関する研究
Title(English)	A study on practical attribute-based encryption and signature
著者(和文)	冨田斗威
Author(English)	Toi Tomita
出典(和文)	学位:博士(工学), 学位授与機関:東京工業大学, 報告番号:甲第11759号, 授与年月日:2022年3月26日, 学位の種別:課程博士, 審査員:尾形 わかは,植松 友彦,山田 功,松本 隆太郎,田中 圭介
Citation(English)	Degree:Doctor (Engineering), Conferring organization: Tokyo Institute of Technology, Report number:甲第11759号, Conferred date:2022/3/26, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	要約
Type(English)	Outline

A Study on Practical Attribute-based Encryption and Signature

Toi Tomita

Supervisor: Professor Wakaha Ogata

Department of Information and Communications Engineering
School of Engineering
Tokyo Institute of Technology

Outline

Recent advances in computation and technology, such as the widespread use of cloud services and the development of artificial intelligence technology, have had a significant impact on our society and our lives. By storing sensitive information such as personal information in the cloud and utilizing it, we can create new value. On the other hand, storing such sensitive information in the cloud poses a security threat. Traditional public-key cryptography can be used to keep the data secret and to guarantee the integrity of the data. However, it lacks the expressive power to realize more advanced functionalities envisioning complex utilization and applications of data.

To solve these problems, research on advanced cryptography has been a major trend in the community of cryptography. Advanced cryptography is a general term for cryptography with advanced additional functionalities that are not available in traditional cryptography, and various advanced cryptographic protocols have been proposed so far. However, most of them are only theoretically interested in "Can we realize the scheme?" and the research on practical advanced cryptography is still considered insufficient. Here, practical means simultaneously having high efficiency, strong security, and a wide range of functionality.

In this thesis, we focus on attribute-based encryption and attribute-based signature, which are advanced cryptography, and address the realization of practical attribute-based encryption and attribute-based signature schemes.

Attribute-Based Encryption

Attribute-based encryption (ABE) [SW05, GPSW06] is an advanced form of public-key encryption to support fine-grained access control for encrypted data. In ABE, ciphertexts and secret keys are associated with descriptive values that determine whether decryption is possible. In a ciphertext-policy ABE (CP-ABE), ciphertexts are associated with access policies like ((department:human resources) AND (position:manager)) OR (position:director), and secret keys are associated with attributes like {(department:human resources), (position:manager)}, and decryption is possible only when the attributes satisfy the access policy. A key-policy ABE (KP-ABE) is the dual of CP-ABE with ciphertexts associated with policy and secret keys associated with attributes. In contrast to ordinary public-key encryption, in which the sender encrypts the message to a specific recipient, ABE allows the sender to specify more flexibly who can read the message.

The most basic security notion for ABE is INDistinguishability against Chosen-Plaintext Attacks (IND-CPA), which captures passive, eavesdropping attacks. IND-CPA security for ABE ensures that information about the encrypted data is not revealed to an adversary who has multiple secret keys that cannot individually decrypt the target ciphertext. The de fact

security notion for ABE is a stronger so-called IND-CCA2, that stands for INDistinguishability against adaptive Chosen-Ciphertexts Attacks, where the adversary can actively manipulate and tamper with ongoing ciphertexts. Such attacks are feasible in practice, as in the attack by [Ble98] against a widely used cryptographic protocol. Traditional security notions such as IND-CPA/IND-CCA2 for ABE implicitly assume that the secret keys, which can decrypt the target ciphertext, are completely hidden from an adversary. However, in real life, an adversary may learn some partial information on the secret keys by side-channel attacks [KJJ99] or by cold-boot attacks [HSH+08].

To tackle this problem, Akavia et al. [AGV09] introduced the bounded memory leakage (BML) model and formulated leakage-resilient CPA (LR-CPA) security of PKE schemes. Soon after, Naor and Segev [NS09] defined LR-CCA2 security. In the BML model, the total amount of key leakage is bounded. Brakerski et al. [BKKV10] and Dodis et al. [DHLW10a] independently introduced the continual memory leakage (CML) model, where there is a notion of time periods and secret keys are updated at the end of each time period. In the CML model, an adversary is allowed to obtain a limited amount of leakage of secret keys in each time period, but there is no limitation on the total amount of leakage that the adversary obtained in all time periods. An LR-CPA/CCA2-secure PKE scheme in the BML or CML model is IND-CPA/CCA2-secure even if partial information of the secret key within the range allowed by each model is leaked to the adversary.

We can also consider the leakage-resilient (LR) security model of ABE schemes [AGV09, LRW11]. Indeed, many efficient LR-CPA-secure ABE schemes have been constructed so far [CDRW10, KP13, YAX+16, ZCG+18].

To achieve LR-CCA2-security, there exists a generic method to transform any LR-CPA-secure ABE schemes to LR-CCA2-secure ones based on the Naor-Yung double encryption paradigm [NY90]. The resulting scheme is, however, very inefficient because this method uses a simulation-sound NIZK [NS09, ADN+10] or a true simulation extractable NIZK [DHLW10b] in addition to doubling the original (CPA) ciphertext.

Unfortunately, the generic construction is the only known method to construct an LR-CCA2-secure ABE scheme except for special cases like identity-based encryption (IBE). A natural question arises:

(Q1) Can we construct efficient LR-CCA2-secure ABE schemes?

Next, we focus on IBE. Several LR-CCA2-secure IBE schemes [ADN+10, SGL14, LTZY16, CQX18], which are more efficient than the generic construction, have been proposed. Unfortunately, all these LR-CCA2-secure IBE schemes rely on q-type assumptions. Note that q-type assumptions are dynamic assumptions, in which the complexity of the assumptions depends on a certain parameter q determined by the behavior of the adversary. It is known that many q-type assumptions become stronger as q grows [Che06], and in general, such complex and dynamic assumptions are not well-understood. Thus, it is better to avoid such q-type assumptions. Therefore, a question that we are interested in is:

(Q2) Can we construct efficient LR-CCA2-secure IBE schemes without q*-type assumptions?*

Very recently, several LR-CCA2-secure IBE schemes without q-type assumptions have been proposed (e.g., [ZYXM19]). However, to the best of our knowledge, no scheme is secure if more than half of the secret key is leaked. It has been shown that a cold boot attack can

leak a significant fraction of the secret key. Thus, for real-life applications, it is desirable that the security of the cryptographic protocol is not compromised even if most of the secret key is leaked. Therefore, we also consider the following problem:

(Q3) Can we construct efficient LR-CCA2-secure IBE schemes that allow leakage of most of the secret key?

Contributions

We give positive answers to the above questions as follows.

Contribution 1.1: LR-CCA2-secure IBE scheme without q-type assumptions

First, we propose the first LR-CCA2-secure IBE scheme that does not depend on q-type assumptions. Namely, the proposed scheme is secure under the external Matrix Decisional Diffie-Hellman (exMDDH) assumption, which is a kind of well-studied assumption. This is the positive answer to (Q2). The exMDDH assumption is parametrized by $k \in \{2, 3, \ldots\}$, and k can be chosen freely. The smaller k we choose, the more efficient and the larger the allowed leakage rate the scheme has, while the stronger assumption we need.

To obtain our result, we construct an LR-CCA2-secure identity-based key-encapsulation mechanism (IBKEM). An LR-CCA2-secure IBE scheme is obtained by combining our IBKEM scheme with any CCA2-secure symmetric-key encryption scheme (which does not need to be leakage-resilient). Our LR-CCA2-secure IBKEM scheme is obtained by applying the technique of Qin et al. [QCL14] to the LR-CPA-secure IBE scheme of Kurosawa and Phong [KP13].

We show a comparison of LR-CCA2-secure IBE schemes in Table 1. Here, the leakage rate is defined as the ratio of the amount of allowed leakage to the secret key size.

Table 1: Comparison of LR-CCA2-secure IBE schemes.

Schemes	Assumption	Leakage rate
Alwen et al. [ADN+10]	q-type	1/6
Sun et al. [SGL14]	q-type	1/6
Li et al. [LTZY16]	q-type	1/4
Chen et al.[CQX18]	q-type	1/2
Ours	k-exMDDH	$1/(4k+2)$

Contribution 1.2: LR-CCA2-secure ABE schemes

Next, we give positive answers to the above questions (Q1) and (Q3). We develop new LR-CCA2-secure ABE schemes that are more efficient than the generic construction. Our schemes are obtained by boosting the LR-CPA-security of some existing schemes [KP13, ZCG+18] to the LR-CCA2-security. The schemes are almost as efficient as the underlying LR-CPA-secure schemes, and in particular, each ciphertext is only 2 group elements larger than those of the underlying schemes. We summarize our results below.

1. We construct the first LR-CCA2-secure ABE schemes for a large class of predicates. Our ABE scheme allows its master secret key leakage and user's secret key leakage

in the CML model. By combining with [ZCG+18], we obtain the following concrete LR-CCA2-secure ABE schemes:

- Inner-product encryption (IPE) and non-zero IPE,
- (Doubly) spatial encryption,
- KP-ABE and CP-ABE for boolean formulae,
- KP-ABE and CP-ABE for arithmetic formulae,
- Broadcast encryption.

The leakage rates of the above LR-CCA2-secure ABE schemes are the same as the LR-CPA-secure one of [ZCG+18].

2. We construct the first LR-CCA2-secure IBE scheme with optimal leakage rate. *Optimal* leakage rate means that the leakage rate can be arbitrarily close to 1 by setting parameters appropriately. More specifically, our IBE scheme is resilient to the leakage of $(1 - o(1))$-fraction of its user's secret key in the BML model, but does not allow its master key leakage.

To obtain our results, we develop a new quasi-adaptive non-interactive zero-knowledge (QA-NIZK) argument for the ciphertext consistency of the LR-CPA-secure schemes. Our new QA-NIZK argument has simulation-soundness and a small proof, that allows us to boost LR-CPA-security to LR-CCA2-security efficiently.

A QA-NIZK argument is an NIZK argument in which a common reference string depends on the language. We develop the first simulation-sound QA-NIZK argument for a language that is characterized by *generalized* tagged linear subspaces (GTLS), that is defined as

$$\mathcal{L}_{\rho}^{\mathsf{GTLS}} := \{([\mathbf{c}], \mathbf{x}) \mid \exists \mathbf{r} \in \mathbb{Z}_q^t \text{ s.t. } \mathbf{c} = \mathbf{M}_{\mathbf{x}}\mathbf{r}\}, \tag{1}$$

where $\rho := ([\mathbf{M}], [\mathbf{M}'_1], \ldots, [\mathbf{M}'_m]) \in \mathbb{G}^{n\times t} \times (\mathbb{G}^{n'\times t})^m$, $n > t$, $n' \geq 1$, x_i is the i-th element of $\mathbf{x} \in \mathbb{Z}_q^m$, and $\mathbf{M}_{\mathbf{x}} := \begin{pmatrix} \mathbf{M} \\ \sum_{i=1}^m x_i \mathbf{M}'_i \end{pmatrix}$. (We use implicit representation of group elements as in [EHK+13].) Previously, the simulation-sound QA-NIZK argument is known only for $m = 0$ (linear subspaces). No-simulation-sound QA-NIZK argument is known for $m = 2$ and $x_1 = 1$ (tagged linear subspaces). We also show that a QA-NIZK argument for the above language implies one for the following language:

$$\hat{\mathcal{L}}_{\rho}^{\mathsf{GTLS}} := \{([\mathbf{c}], L) \mid \exists \mathbf{r} \in \mathbb{Z}_q^t \text{ s.t. } \mathbf{c} = \mathbf{M}_L\mathbf{r}\}, \tag{2}$$

where L is a linear map and $\mathbf{M}_L := \begin{pmatrix} \mathbf{M} \\ L(\mathbf{M}'_1, \ldots, \mathbf{M}'_m) \end{pmatrix}$. We summarize the differences between our QA-NIZK argument and the existing ones in Table 2.

We believe that our new QA-NIZK argument has other applications because it supports more general languages than languages for just linear subspaces.

Technical Overview

Here, we provide overview of our techniques.

Table 2: Comparison of QA-NIZK arguments. The schemes in the column of $m = 0$ are a QA-NIZK argument for just linear subspaces, and the schemes in the column of $m \geq 1$ are a QA-NIZK argument for (generalized) tagged linear subspaces.

	Linear subspaces ($m = 0$)	Tagged linear subspaces ($m \geq 1$)
No-simulation-sound	Already exist, e.g. JR13 [JR13]	Already exist, e.g. JR13 [JR13]
Simulation-sound	Already exist, e.g. KW15 [KW15]	**Ours**

How to boost CPA to CCA2 for leakage-resilient ABE. As mentioned above, we can obtain LR-CCA2-secure schemes from LR-CPA-secure schemes through the Naor-Yung paradigm [NY90]. The resulting scheme is, however, very inefficient.

In [JR14, LPJY14, LPJY15], the authors constructed CCA2-secure PKE schemes by using an efficient simulation-sound QA-NIZK argument for linear subspaces. In these PKE schemes, the ciphertext consistency can be verified by a linear equation, that depends only on a public key. In the case of ABEs, however, the consistency check equation depends not only on the public parameter (which is a fixed parameter) but also on the attribute (which is a variable). Therefore, we cannot use existing (simulation-sound) QA-NIZK arguments for linear subspaces to construct LR-CCA2-secure ABE schemes in general.

On the other hand, in [HJP18, LP20a, LP20b], the authors showed a CPA-to-CCA2 transformation for (not leakage-resilient) IBE schemes by using a simulation-sound (tag-based) QA-NIZK argument for linear subspaces. At first glance, thanks to the public verifiability of the QA-NIZK argument, their approach seems to provide LR-CCA2-secure schemes by only replacing the CPA-secure schemes with LR-CPA-secure ones. Unfortunately, it does not work well, because the proof of the (non-LR) CCA2-security in their approach makes use of the property that a secret key is uniformly random from the adversary's view point. In the LR-security model, the adversary can learn partial knowledge about the secret key, and hence we cannot ensure the uniform randomness of it.

From the above discussion, it is difficult to construct LR-CCA2-secure ABE schemes by using the existing very efficient QA-NIZK schemes. We solve this problem by developing a new simulation-sound QA-NIZK argument.

How to achieve simulation-sound QA-NIZK argument for GTLS. Our *simulation sound* QA-NIZK argument for *generalized tagged linear subspaces (GTLS)* is obtained as a (non-trivial) combination of the QA-NIZK arguments by Jutla and Roy [JR13] and by Kiltz and Wee [KW15]. The former is *no simulation sound* one for *tagged linear subspaces* and the latter is a *simulation sound* one for *linear subspaces*. Our main observation is to consider designated verifier (DV) variants of these two QA-NIZK arguments. Then their security proofs are greatly simplified, and we find out that these arguments have a close relationship. This observation allows us to construct the first *simulation-sound* QA-NIZK argument for *generalized tagged* linear subspaces.

More details are as follows. The language for tagged linear subspaces is defined as follows:

$$\mathcal{L}_{\rho}^{\mathsf{tagged}} := \{([\mathbf{c}], x) \mid \exists \mathbf{r} \in \mathbb{Z}_q^t \text{ s.t. } \mathbf{c} = \mathbf{M}_x \mathbf{r}\}, \tag{3}$$

where $\rho := ([\mathbf{M}], [\mathbf{M}'_0], [\mathbf{M}'_1])$ and $\mathbf{M}_x := \begin{pmatrix} \mathbf{M} \\ \mathbf{M}'_0 + x\mathbf{M}'_1 \end{pmatrix}$. In the DV variant of Jutla-Roy's scheme, a verifier has a secret verification key which is random vectors $\mathbf{k} \in \mathbb{Z}_q^{n'}$ and $\mathbf{k}_0, \mathbf{k}_1 \in \mathbb{Z}_q^n$,

and the common reference string (CRS) is the projections $[\mathbf{p}_0] := [\mathbf{M}^\top \mathbf{k}_0 + \mathbf{M}_0'^\top \mathbf{k}]$ and $[\mathbf{p}_1] := [\mathbf{M}^\top \mathbf{k}_1 + \mathbf{M}_1'^\top \mathbf{k}]$. To prove that $([\mathbf{c}], x)$ satisfies $[\mathbf{c}] = [\mathbf{M}_x \mathbf{r}]$ for some $\mathbf{r} \in \mathbb{Z}_q^t$, the prover outputs $\pi := [\mathbf{r}^\top(\mathbf{p}_0 + x\mathbf{p}_1)]$ as a proof. With the verification key, the (designated) verifier can check whether $\pi = [\mathbf{c}^\top \mathbf{k}_x]$, where $\mathbf{k}_x := \begin{pmatrix} \mathbf{k}_0 + x\mathbf{k}_1 \\ \mathbf{k} \end{pmatrix}$. By using $\mathbf{k}$, $\mathbf{k}_0$, and $\mathbf{k}_1$ as a simulation trapdoor, a simulated proof is given by $\tilde{\pi} := [\mathbf{c}^\top \mathbf{k}_x]$. Perfect completeness and zero-knowledge follow from the following equation:

$$\mathbf{r}^\top(\mathbf{p}_0 + x\mathbf{p}_1) = \mathbf{r}^\top \left(\mathbf{M}^\top(\mathbf{k}_0 + x\mathbf{k}_1) + \left(\mathbf{M}_0'^\top + x\mathbf{M}_1'^\top \right) \mathbf{k} \right) = \mathbf{r}^\top \mathbf{M}_x^\top \mathbf{k}_x = \mathbf{c}^\top \mathbf{k}_x.$$

Soundness is guaranteed by the fact that if $\mathbf{c}$ is outside the span of $\mathbf{M}_x$ for x chosen by an adversary, then $\mathbf{c}^\top \mathbf{k}_x$ is completely random given $\mathbf{M}^\top \mathbf{k}_0 + \mathbf{M}_0'^\top \mathbf{k}$ and $\mathbf{M}^\top \mathbf{k}_1 + \mathbf{M}_1'^\top \mathbf{k}$.

Now we observe that this scheme has similar structure to the DV variant of Kiltz-Wee's scheme. Therefore, by using their techniques, the scheme can be converted to a *simulation-sound* and *publicly-verifiable* QA-NIZK argument.

The above QA-NIZK argument is a special case of a QA-NIZK argument for the *generalized* tagged linear subspaces (GTLS) given by Eq. (1), where $m = 2$ and $x_1 = 1$. We further show that this argument can be extended to the GTLS in this thesis.

By a straightforward encoding, we also demonstrate that a QA-NIZK argument for GTLS implies one for the language in Eq. (2).

Attribute-Based Signature

Attribute-based signature (ABS) [MPR11] is an ambitious variant of digital signature that simultaneously allows fine-grained access control for user authentication and anonymous authentication of messages. In the message-policy ABS (MP-ABS), signing keys are associated with attributes like {(department:human resources), (position:manager)}, and the signer can sign any message with any policy that satisfies the attributes, like (department:human resources) OR (position:director), using the signing key. The key-policy ABS (KP-ABS) is the dual of MP-ABS, where the roles of attributes and policies are swapped. In contrast to ordinary digital signature, with ABS, a signer can sign without revealing the identity or attributes of the signer.

The security requirements of ABS are unforgeability and privacy. Unforgeability of ABS ensures that a valid signature on any message associated with any policy cannot be generated by an adversary who has multiple signing keys associated with attributes that does not satisfy individually the signing policy, like {(department:sales), (position:manager)}. The other requirement, privacy, ensures that information about who the actual signer is and what their attributes are not revealed by the signature.

Over the past decade, a number of ABS schemes have been proposed that achieve different trade-offs between efficiency, security, and assumptions for policy classes of varying expressiveness. On the other hand, ABS has found many applications such as anonymous credential [SS09], attribute-based messaging [MPR11], and secret leaking [MPR11]. The main demand of ABS schemes is efficiency, especially compact signatures. That is, the size of the ABS signature is independent of the size of the attribute and the policy, which are used to sign the message.

ABS scheme with compact signatures is extremely desirable. In practical applications of ABS, where a large number of attributes and large policies are involved for complex access

control, compact signatures are much more preferable. So far, several ABS schemes with compact signatures have been proposed [CCL+13, BGI14, AHY15, NP19]. However, all schemes either rely on less-understood assumptions, provide only weak security, or do not support complex policies.

Contribution: We construct the first KP-ABS scheme with compact signatures simultaneously satisfying the following properties:

1. *Expressiveness:* Supports policies expressed in $\mathbf{NC}^1$ circuits.
2. *Security:* Satisfies strong adaptive security rather than weaker selective security.
3. *Assumption:* Based on well-studied assumptions, not less-studied assumptions including q-type assumptions, decisional subgroup (DSG) assumptions over composite-order groups, knowledge assumptions, indistinguishable obfuscations (iO). Concretely, our scheme is based on the MDDH assumption over prime-order groups.
4. *Efficiency:* Has compact signatures.

We show a comparison of ABS schemes with compact signatures in Table 3, where MSP stands for monotone span programs.

Table 3: Comparison of ABS schemes with compact signatures.

Schemes	Policy	Adaptive	Assumption
[CCL+13]	threshold	✓	q-type
[BGI14]	all circuits	✓	knowledge assumption
[AHY15]	MSP		q-type
[DDM17]	Turing machines		iO
[NP19]	$\mathbf{NC}^1$	✓	DSG
Ours	$\mathbf{NC}^1$	✓	MDDH ✓

To construct an ABS scheme with the above properties, we follow the (non-black-box) ABE-to-ABS conversion, proposed by [OT11], that is somewhat reminiscent of Naor's IBE-to-signature conversion [BF01]. By starting with the KP-ABE scheme with compact ciphertexts by [KNYY20], we obtain the KP constrained signature (CS) scheme with compact signatures. Here, CS is a slightly simplified version of ABS. That is, with KP-CS, a signer signs an "attribute" that satisfies the policy associated with their signing key, but not a "message." From the ABE-to-ABS conversion [OT11], the resulting CS scheme inherits the above-desired properties of the ABE scheme, which are expressiveness, security, and the underlying assumption. To obtain the full-fledged ABS scheme, we combine the resulting CS scheme with the compatible compact signature scheme from the IBE scheme by [BKP14, CGW15]. By signing an attribute in the CS part and signing a message in the signature part, we obtain the full-fledged ABS scheme without losing the desired properties.

Our KP-ABS scheme implies the first message-policy (MP) ABS scheme with compact signatures because we can easily convert KP-ABS into MP-ABS by using universal circuits. In more detail, let $U(\cdot,\cdot)$ be a universal circuit that takes as input a circuit C of fixed depth and size and an input x to the circuit C and outputs $C(x)$. Next, let $U[x]$ be the universal

circuit with the input x hard-wired. Then, we may construct an MP-ABS scheme using a KP-ABS scheme as follows. The signer of MP-ABS, given an attribute x, issued a signing key of KP-ABS for the circuit $U[x]$. Then, the signer signs a message associated with a circuit C by using signing procedure of KP-ABS for the message and the circuit C as $U[x](C) = U(C, x) = C(x)$, where C is viewed as a bit string representing KP-ABS attributes. Verification is straightforward using KP-ABS verification. By using the depth-universal circuit of Cook and Hoover [CH85], the circuit $U[x]$ is also $\mathbf{NC}^1$. Therefore, our KP-ABS scheme can deal the circuit $U[x]$ as a policy.

Bibliography

[ADN+10] Joël Alwen, Yevgeniy Dodis, Moni Naor, Gil Segev, Shabsi Walfish, and Daniel Wichs. Public-key encryption in the bounded-retrieval model. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 113–134. Springer, Heidelberg, May / June 2010. 2, 3

[AGV09] Adi Akavia, Shafi Goldwasser, and Vinod Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 474–495. Springer, Heidelberg, March 2009. 2

[AHY15] Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada. Conversions among several classes of predicate encryption and applications to ABE with various compactness tradeoffs. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 575–601. Springer, Heidelberg, November / December 2015. 7

[BF01] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, Heidelberg, August 2001. 7

[BGI14] Elette Boyle, Shafi Goldwasser, and Ioana Ivan. Functional signatures and pseudorandom functions. In Hugo Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 501–519. Springer, Heidelberg, March 2014. 7

[BKKV10] Zvika Brakerski, Yael Tauman Kalai, Jonathan Katz, and Vinod Vaikuntanathan. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In *51st FOCS*, pages 501–510. IEEE Computer Society Press, October 2010. 2

[BKP14] Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (Hierarchical) identity-based encryption from affine message authentication. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 408–425. Springer, Heidelberg, August 2014. 7

[Ble98] Daniel Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 1–12. Springer, Heidelberg, August 1998. 2

[CCL+13] Cheng Chen, Jie Chen, Hoon Wei Lim, Zhenfeng Zhang, Dengguo Feng, San Ling, and Huaxiong Wang. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. In Ed Dawson, editor, *CT-RSA 2013*, volume 7779 of *LNCS*, pages 50–67. Springer, Heidelberg, February / March 2013. 7

[CDRW10] Sherman S. M. Chow, Yevgeniy Dodis, Yannis Rouselakis, and Brent Waters. Practical leakage-resilient identity-based encryption from simple assumptions. In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *ACM CCS 2010*, pages 152–161. ACM Press, October 2010. 2

[CGW15] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624. Springer, Heidelberg, April 2015. 7

[CH85] Stephen A. Cook and H. James Hoover. A depth-universal circuit. *SIAM J. Comput.*, 14:833–839, 1985. 8

[Che06] Jung Hee Cheon. Security analysis of the strong Diffie-Hellman problem. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 1–11. Springer, Heidelberg, May / June 2006. 2

[CQX18] Yu Chen, Baodong Qin, and Haiyang Xue. Regularly lossy functions and applications. In Nigel P. Smart, editor, *CT-RSA 2018*, volume 10808 of *LNCS*, pages 491–511. Springer, Heidelberg, April 2018. 2, 3

[DDM17] Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay. Short attribute-based signatures for arbitrary turing machines from standard assumptions. Cryptology ePrint Archive, Report 2017/801, 2017. https://ia.cr/2017/801. 7

[DHLW10a] Yevgeniy Dodis, Kristiyan Haralambiev, Adriana López-Alt, and Daniel Wichs. Cryptography against continuous memory attacks. In *51st FOCS*, pages 511–520. IEEE Computer Society Press, October 2010. 2

[DHLW10b] Yevgeniy Dodis, Kristiyan Haralambiev, Adriana López-Alt, and Daniel Wichs. Efficient public-key cryptography in the presence of key leakage. In Masayuki Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 613–631. Springer, Heidelberg, December 2010. 2

[EHK+13] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, August 2013. 4

[GPSW06] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 2006*, pages 89–98. ACM Press, October / November 2006. Available as Cryptology ePrint Archive Report 2006/309. 1

[HJP18] Dennis Hofheinz, Dingding Jia, and Jiaxin Pan. Identity-based encryption tightly secure under chosen-ciphertext attacks. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 190–220. Springer, Heidelberg, December 2018. 5

[HSH+08] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: Cold boot attacks on encryption keys. In Paul C. van Oorschot, editor, *USENIX Security 2008*, pages 45–60. USENIX Association, July / August 2008. 2

[JR13] Charanjit S. Jutla and Arnab Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20. Springer, Heidelberg, December 2013. 5

[JR14] Charanjit S. Jutla and Arnab Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 295–312. Springer, Heidelberg, August 2014. 5

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 388–397. Springer, Heidelberg, August 1999. 2

[KNYY20] Shuichi Katsumata, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. Compact NIZKs from standard assumptions on bilinear maps. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 379–409. Springer, Heidelberg, May 2020. 7

[KP13] Kaoru Kurosawa and Le Trieu Phong. Leakage resilient IBE and IPE under the DLIN assumption. In Michael J. Jacobson Jr., Michael E. Locasto, Payman Mohassel, and Reihaneh Safavi-Naini, editors, *ACNS 13*, volume 7954 of *LNCS*, pages 487–501. Springer, Heidelberg, June 2013. 2, 3

[KW15] Eike Kiltz and Hoeteck Wee. Quasi-adaptive NIZK for linear subspaces revisited. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128. Springer, Heidelberg, April 2015. 5

[LP20a] Roman Langrehr and Jiaxin Pan. Hierarchical identity-based encryption with tight multi-challenge security. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 153–183. Springer, Heidelberg, May 2020. 5

[LP20b] Roman Langrehr and Jiaxin Pan. Unbounded HIBE with tight security. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 129–159. Springer, Heidelberg, December 2020. 5

[LPJY14] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure

encryption from homomorphic signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 514–532. Springer, Heidelberg, May 2014. 5

[LPJY15] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Compactly hiding linear spans - tightly secure constant-size simulation-sound QA-NIZK proofs and applications. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 681–707. Springer, Heidelberg, November / December 2015. 5

[LRW11] Allison B. Lewko, Yannis Rouselakis, and Brent Waters. Achieving leakage resilience through dual system encryption. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 70–88. Springer, Heidelberg, March 2011. 2

[LTZY16] Jiguo Li, Meilin Teng, Yichen Zhang, and Qihong Yu. A Leakage-Resilient CCA-Secure Identity-Based Encryption Scheme. *The Computer Journal*, 59(7):1066–1075, 07 2016. 2, 3

[MPR11] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-based signatures. In Aggelos Kiayias, editor, *CT-RSA 2011*, volume 6558 of *LNCS*, pages 376–392. Springer, Heidelberg, February 2011. 6

[NP19] Mridul Nandi and Tapas Pandit. Predicate signatures from pair encodings via dual system proof technique. *Journal of Mathematical Cryptology*, 13, 07 2019. 7

[NS09] Moni Naor and Gil Segev. Public-key cryptosystems resilient to key leakage. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 18–35. Springer, Heidelberg, August 2009. 2

[NY90] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *22nd ACM STOC*, pages 427–437. ACM Press, May 1990. 2, 5

[OT11] Tatsuaki Okamoto and Katsuyuki Takashima. Efficient attribute-based signatures for non-monotone predicates in the standard model. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 35–52. Springer, Heidelberg, March 2011. 7

[QCL14] Baodong Qin, Kefei Chen, and Shengli Liu. Efficient chosen-ciphertext secure public-key encryption scheme with high leakage-resilience. *IET Information Security*, 9, 01 2014. 3

[SGL14] Shifeng Sun, Dawu Gu, and Shengli Liu. Efficient leakage-resilient identity-based encryption with CCA security. In Zhenfu Cao and Fangguo Zhang, editors, *PAIRING 2013*, volume 8365 of *LNCS*, pages 149–167. Springer, Heidelberg, November 2014. 2, 3

[SS09] Siamak Fayyaz Shahandashti and Reihaneh Safavi-Naini. Threshold attribute-based signatures and their application to anonymous credential systems. In

Bart Preneel, editor, *AFRICACRYPT 09*, volume 5580 of *LNCS*, pages 198–216. Springer, Heidelberg, June 2009. 6

[SW05] Amit Sahai and Brent R. Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, Heidelberg, May 2005. 1

[YAX+16] Zuoxia Yu, Man Ho Au, Qiuliang Xu, Rupeng Yang, and Jinguang Han. Leakage-resilient functional encryption via pair encodings. In Joseph K. Liu and Ron Steinfeld, editors, *ACISP 16, Part I*, volume 9722 of *LNCS*, pages 443–460. Springer, Heidelberg, July 2016. 2

[ZCG+18] Jie Zhang, Jie Chen, Junqing Gong, Aijun Ge, and Chuangui Ma. Leakage-resilient attribute based encryption in prime-order groups via predicate encodings. *Designs, Codes and Cryptography*, 86(6):1339–1366, 2018. 2, 3, 4

[ZYXM19] Yanwei Zhou, Bo Yang, Zhe Xia, and Yi Mu. Identity-based encryption with leakage-amplified chosen-ciphertext attacks security. *Theoretical Computer Science*, 809, 12 2019. 2