1Y-1

Generic Constructions of Public-Key Encryption in the Presence of Key Leakage

Manh Ha Nguyen [*] [†] Kenji Yasunaga [†] Keisuke Tanaka [†]

1 Background

Key-leakage attacks. The introduction of memory attacks (or "cold boot attacks") by Halderman et al. [5], gave rise to the notion of *leakage resiliency*, presented by Akavia, Goldwasser and Vaikuntanathan [1] and further explored by Naor and Segev [6]. In their definition, security holds even if the attacker gets some information of its choosing (depending on the value of the public-key) on the scheme's secret key, with the only restriction that the total amount of leakage is bounded. Public-key encryption schemes presenting in [1, 6] are resilent to leakage of even $1 - o(1)$ fraction of secret key (we call this the "leakage rate").

Naor and Segev [6] extended the framework of key leakage to the setting of chosen-ciphertext attacks. On the theoretical side, they proved that the Naor-Yung paradigm is applicable in this setting as well, and obtained as a corollary encryption schemes that are CCA2-secure with the leakage rate of $1-o(1)$. On the practical side, they proved that variants of the Cramer-Shoup cryptosystem are CCA1-secure with the leakage rate of $1/4$, and CCA2-secure with the leakage rate of $1/6$.

Stateful public-key encryption (StPE). In 2006, Bellare et al. [2] proposed the model of a StPE scheme $\mathbf{StPE}$ = (Setup, KG, PKCk, NwSt, Enc, Dec). It is specified by six algorithms (all possibly randomized except the last) whose operation is illustrated in [2, Figure 2]. The approach that they adopt to construct StPE schemes is to convert specific public-key encryption schemes such as DHIES and Kurosawa and Desmedts hybrid encryption scheme into StPE schemes.

In 2008, Baek et al. [3] presented generic constructions of StPE, built several new StPE schemes and explained existing ones using their generic constructions.

2 Contributions

In the paper [6], Naor et al. proved that a variant of the Cramer-Shoup cryptosystem [4] is secure against a-posteriori chosen-ciphertext (CCA2) and key-leakage attacks. This CCA2-secure scheme is based on the hardness of the DDH problem. From this idea and the idea of building generic constructions of StPE presented by Baek et al. [3], we make the following contributions in this paper:

1. We present a generic construction of a stateless public-key encryption that is resilient to chosen-ciphertext and key-leakage attacks. In this construction, we use the combination of any 1-universal hash proof system that satisfies the condition of a key-leakage extractor and any 2-universal hash proof system with some condition on the length of proof.

2. We also present a generic construction of a StPE that is resilient to chosen-ciphertext and key-leakage attacks. In this construction, we use the combination of 2 hash proof systems as in the case of stateless public-key encryption and any IND-CCA-secure symmetric encryption.

3 Generic Constructions from Hash Proof Systems

Hash proof systems. A hash proof system HPS = *(KGen, Pub, Priv)* consists of three algorithms that run in polynomial time. The algorithm Pub receives as input a public key pk, a valid ciphertext $x \in L$, and a witness w of the fact that $x \in L$, and outputs the encapsulated key $\pi \in \mathbf{\Pi}$ (where $\mathbf{\Pi}$ denotes the set of encapsulated symmetric keys). The algorithm $Priv$ receives as input a secret key sk and a valid ciphertext $x \in L$, and outputs the encapsulated key π. We say that a hash proof system is 1-universal if for all possible outcomes of $KGen(1^n)$ it holds that

$$\Delta((pk, \pi), (pk, \mathrm{U}(\mathbf{\Pi}))) \leq \epsilon$$

where $\mathrm{U}(\mathbf{\Pi}) \in \mathbf{\Pi}$ is sampled uniformly at random.

Definition 3.1. *We say that a hash proof system* HPS = *(KGen, Pub, Priv) for a language L is a 1-universal (λ, ϵ)-key-leakage extractor if for any function $f : \{0,1\}^* \to \{0,1\}^\lambda$ we have*

$$\Delta((pk, x, f(sk), Priv(x, sk)), (pk, x, f(sk), U(\mathbf{\Pi}))) \leq \epsilon$$

where $x \in_R X$. If $\epsilon = negl(n)$ we say that HPS *is a 1-universal λ-key-leakage extractor for L.*

3.1 Stateless Public-Key Encryption

Let $\mathbf{HPS}_1 = (KGen_1, Pub_1, Priv_1)$ be a 1-universal HPS for a language L, and $\mathbf{HPS}_2 = (KGen_2, Pub_2, Priv_2)$ be a 2-universal HPS for the same language L. We define an encryption scheme $\Pi = (KGen, Enc, Dec)$ as follows:

* Supported by Ministry of Education, Culture, Sports, Science and Technology.

† Department of Mathematical and Computing Sciences, Tokyo Institute of Technology. W8-55, 2-12- 1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan. {nguyen9, yasunaga, keisuke}@is.titech.ac.jp. This research was supported in part by NTT Information Sharing Platform Laboratories and JSPS Global COE program Computationism as Foundation for the Sciences.

Key Generation : On input 1^n for $n \in \mathbb{Z}_{\geq 0}$

Choose $(pk_1, sk_1) \leftarrow KGen_1(1^n)$, $(pk_2, sk_2) \leftarrow KGen_2(1^n)$.

Output $pk = (pk_1, pk_2)$, $sk = (sk_1, sk_2)$.

Encryption: On input a public key $pk = (pk_1, pk_2)$, along with a message $m \in \mathcal{M}$, compute

E0: $(x, w) \xleftarrow{\$} \mathcal{R}_L$ (where $x \in_R L$);

E1: $\pi_1 = Pub_1(pk_1, x, w)$;

E2: $e = m + \pi_1$;

E3: $\pi_2 = Pub_2(pk_2, x, w, e)$;

E4: Output $c = (x, e, \pi_2)$.

Decryption: On input a secret key $sk = (sk_1, sk_2)$, and a ciphertext c, do the following.

D0: Parse c as a 3-tuple (x, e, π_2); output $\perp$ if c is not of this form.

D1: Compute $\pi_2' = Priv_2(sk_2, x, e)$.

D2: Test if $\pi_2' = \pi_2$; output $\perp$ and halt if this is not the case.

D3: Compute $\pi_1 = Priv_1(sk_1, x)$.

D4: Output $m = e - \pi_1$.

Theorem 3.2. *Assume that L is a membership indistinguishable language,* $\mathbf{HPS}_1$ *is a 1-universal* λ*-key-leakage extractor for L, and* $\mathbf{HPS}_2$ *is a 2-universal HPS for L, with proofs* π_2 *of size* $|\pi_2| = p \geq \lambda + \omega(log(n))$. *Then the encryption scheme constructed from* $\mathbf{HPS}_1$, $\mathbf{HPS}_2$ *is semantically secure against* λ*-key-leakage CCA2 attacks, where n denotes the security parameter.*

3.2 Stateful Public-Key Encryption

Let $\mathbf{HPS}_1$ and $\mathbf{HPS}_2$ as in the case of stateless public-key encryption, **SYM** be a IND-CCA symmetric encryption. We assume that the HPS scheme $\mathbf{HPS}_1$ and the symmetric encryption scheme **SYM** are "compatible" meaning that the key space $\mathcal{K}_K$ of $\mathbf{HPS}_1$ is the same as the key space $\mathcal{K}_D$ of **SYM**.

We define a StPE scheme $\mathbf{StPE}$ as follows:

StPE.KGen: On input sp, do the following.

Choose $(pk_1, sk_1) \leftarrow KGen_1(1^n)$, $(pk_2, sk_2) \leftarrow KGen_2(1^n)$.

Output $PK = (pk_1, pk_2)$, $SK = (sk_1, sk_2)$.

StPE.Enc: On input a public key $PK = (pk_1, pk_2)$, a state st, along with a message $m \in \mathcal{M}$, do the following.

If st is of the form (x, w) of of the form $(x, w, PK'$, $\Pi_1')$ such that $PK' \neq PK$ then compute $\pi_1 = Pub_1($ $pk_1, x, w)$;
Else, Parse st as (x, w, PK, π_1),

E1: $\pi_1 = Pub_1(pk_1, x, w)$;

E2: $e = \mathbf{SYM}.\mathbf{Enc}(\pi_1, m)$;

E3: $\pi_2 = Pub_2(pk_2, x, w, e)$;

E4: Output $c = (x, e, \pi_2)$, and the new state $st = (x, w, PK, \pi_1)$.

StPE.Dec: On input a system parameter sp, a secret key $SK = (sk_1, sk_2)$, a ciphertext c, do the following.

D0: Parse c as a 3-tuple (x, e, π_2); output $\perp$ if c is not of this form.

D1: Compute $\pi_2' = Priv_2(sk_2, x, e)$.

D2: Test if $\pi_2' = \pi_2$; output $\perp$ and halt if this is not the case.

D3: Compute $\pi_1 = Priv_1(sk_1, x)$.

D4: Output $m = \mathbf{SYM}.\mathbf{Dec}(\pi_1, e)$.

Theorem 3.3. *Assume that L is a membership indistinguishable language,* $\mathbf{HPS}_1$ *is a 1-universal* λ*-key-leakage extractor for L,* $\mathbf{HPS}_2$ *is a 2-universal HPS for L, with proofs* π_2 *of size* $|\pi_2| = p \geq \lambda + \omega(log(n))$*, and the underlying symmetric encryption* **SYM** *is IND-CCA secure. Then in the KSK model, the proposed generic stateful public-key encryption scheme* **StPE** *is semantically secure against* λ*-key-leakage CCA2 attacks. More precisely, we have*

$$\mathbf{Adv}^{\mathrm{KL,CCA2}}_{\Pi,A}(n) \leq \mathbf{Adv}^{\mathrm{IND-CCA}}_{B,\mathbf{SYM}}(n),$$

where n denotes the security parameter.

References

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks," In *Proc. of the 6th Theory of Cryptography Conference, TCC '09, LNCS 5444*, Pages 474-495, Springer-Verlag, 2009.

[2] M. Bellare, T. Kohno and V. Shoup, "Stateful Public-Key Cryptosystems: How to Encryption with One 160-bit Exponentiaton," In *ACM-CCS '06*, Pages 380-389, ACM Press, 2006.

[3] J. Baek, J. Zhou and F. Bao, "Generic Construction of Stateful Key Encryption and Their Applications," In *Proc. of the 6th International Conference on Applied Cryptography and Network Security, LNCS 5037*, Pages 75-93, Springer-Verlag, 2008.

[4] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack," In *SIAM Journal on Computing*, Pages 167-226, 2003.

[5] A. Halderman, D.Schoen, N. Heninger, W. Clarkson, W. Paul, A. Calandrino, J. Feldman, J. Appelbaum, and W. Felten, "Lest we remember: Cold boot attack on encryption keys," In*Paul C. Van Oorschot editor, USENIX Security Symposium*, Pages 45-60, USENIX, 2008.

[6] M. Naor and G. Segev,"Public-key cryptosystems resilient to key leakage," In *CRYPTO '09, LNCS 5677*, Pages 1835, Springer-Verlag, 2009.