On the Impossibility of Constructing Efficient KEMs and Programmable Hash Functions in Prime Order Groups

Goichiro Hanaoka, Takahiro Matsuda, Jacob C.N. Schuldt

Research Institute for Secure Systems (**RISEC**)
National Institute of Advanced Industrial Science and Technology (**AIST**)

CRYPTO'12

23/8/2012

Public Key Encryption

- The construction of efficient and (IND-CCA) secure public key encryption has been a successful research area
- Practical and efficient design approach: hybrid encryption
  - A public key encryption scheme is constructed from two components:
    1. A key encapsulation mechanism (KEM)
    2. A data encapsulation mechanism (DEM)

Hybrid Encryption

- Key encapsulation mechanism:

$$1^\lambda \longrightarrow \boxed{\mathsf{KG}} \longrightarrow (pk, sk)$$

$$pk \longrightarrow \boxed{\mathsf{Enc}} \longrightarrow (c, K)$$

$$(sk, c) \longrightarrow \boxed{\mathsf{Dec}} \longrightarrow K/\perp$$

- Data encapsulation mechanism:

$$(K, m) \longrightarrow \boxed{\mathsf{DEnc}} \longrightarrow c'$$

$$(c', K) \longrightarrow \boxed{\mathsf{DDec}} \longrightarrow m$$

Hybrid Encryption

- Key encapsulation mechanism:

$$1^\lambda \longrightarrow \boxed{\mathsf{KG}} \longrightarrow (pk, sk) \qquad pk \longrightarrow \boxed{\mathsf{Enc}} \longrightarrow (c, K) \qquad (sk, c) \longrightarrow \boxed{\mathsf{Dec}} \longrightarrow K/\perp$$

- Data encapsulation mechanism:

(K, m) $\longrightarrow m$

Security
IND-CCA secure encryption is achieved by

1. IND-CCA KEM + IND-OT-CCA DEM
2. Constrained IND-CCA KEM + AE-OT DEM

Efficient Key Encapsulation Mechanisms

- We focus on the problem of minimizing ciphertext overhead
- A number of very efficient KEMs already exist in the standard model

Scheme	Security	Assumption	Overhead
[CS03]	IND-CCA	DDH	$3\,\lvert\mathbb{G}\rvert$
[HaKu08]	IND-CCA	CDH	$3\,\lvert\mathbb{G}\rvert$
[KD04]	Constrained IND-CCA	DDH	$2\,\lvert\mathbb{G}\rvert$
[HoKi07]	Constrained IND-CCA	DDH	$2\,\lvert\mathbb{G}\rvert$
[HaKu08]	Constrained IND-CCA	DDH	$2\,\lvert\mathbb{G}\rvert$
[Kiltz07]	IND-CCA	GHDH	$2\,\lvert\mathbb{G}\rvert$
[BMW05]	IND-CCA	DBDH	$2\,\lvert\mathbb{G}\rvert$
[CHH+07]	Bounded IND-q-CCA	DDH	$1\,\lvert\mathbb{G}\rvert$

Motivating Question

Question
Is it possible to construct a KEM with a ciphertext overhead of less than two group elements that achieves IND-CCA security in the standard model?

The Cramer-Shoup KEM [CS03]

KG :

$$pk = (g,\ h,\ g^{x_1} h^{y_1},\ g^{x_2} h^{y_2},\ g^{z})$$
$$sk = (x_1,\ x_2,\ y_1,\ y_2,\ z)$$

Enc :

Let $pk = (g,\ h,\ X,\ Y,\ Z)$

$c = (g^r,\ h^r,\ (X^\alpha Y)^r)$ $\qquad \alpha = H(g^r, h^r)$

$K = Z^r$

Dec :

Let $c = (c_1,\ c_2,\ c_3)$

If $c_1^{x_1+y_1\alpha} c_2^{x_2+y_2\alpha} = c_3$ $\qquad$ return $K = c_1^z$

Otherwise return $\perp$

The Cramer-Shoup KEM [CS03]

KG :

$$pk = (g,\ h,\ g^{x_1} h^{y_1},\ g^{x_2} h^{y_2},\ g^{z})$$
$$sk = (x_1,\ x_2,\ y_1,\ y_2,\ z)$$

Enc :

Let $pk = (g,\ h,\ X,\ Y,\ Z)$

$c = (g^r,\ h^r,\ H'((X^{\alpha} Y)^r)) \quad \alpha = H(g^r, h^r)$

$K = Z^r$

Dec :

Let $c = (c_1,\ c_2,\ c_3)$

If $H'(c_1^{x_1+y_1\alpha} c_2^{x_2+y_2\alpha}) = c_3$ return $K = c_1^z$

Otherwise return $\perp$

The Hofheinz-Kiltz KEM [HK07]

KG : $pk = (g,\ g^x,\ g^y,\ g^z)$
$sk = (x,\ y,\ z)$

Enc : Let $pk = (g,\ X,\ Y,\ Z)$
$c = (g^r,\ (X^\alpha Y)^r)$ $\qquad \alpha = H(g^r)$
$K = Z^r$

Dec : Let $c = (c_1,\ c_2)$
If $c_1^{x\alpha+y} = c_2$ $\quad$ return $\quad K = c_1^z$
Otherwise return $\perp$

The Hofheinz-Kiltz KEM [HK07]

KG :

$$pk = (g,\ g^x,\ g^y,\ g^z)$$
$$sk = (x,\ y,\ z)$$

Enc :

Let $pk = (g,\ X,\ Y,\ Z)$

$c = (g^r,\ H'((X^\alpha Y)^r))$ $\quad \alpha = H(g^r)$

$K = Z^r$

Dec :

Let $c = (c_1,\ c_2)$

If $H'(c_1^{x\alpha+y}) = c_2$ return $K = c_1^z$

Otherwise return $\perp$

Main Result

- We show that
    - There is no algebraic black-box reduction from the OW-CCA security of a class of KEMs with ciphertexts consisting of a single group element and a string, to the hardness of a non-interactive problem

A Class of Efficient Key Encapsulation Mechanisms

- We consider a class $\mathcal{K}$ of KEMs defined in a prime order group $\mathbb{G}$ with the following additional properties:

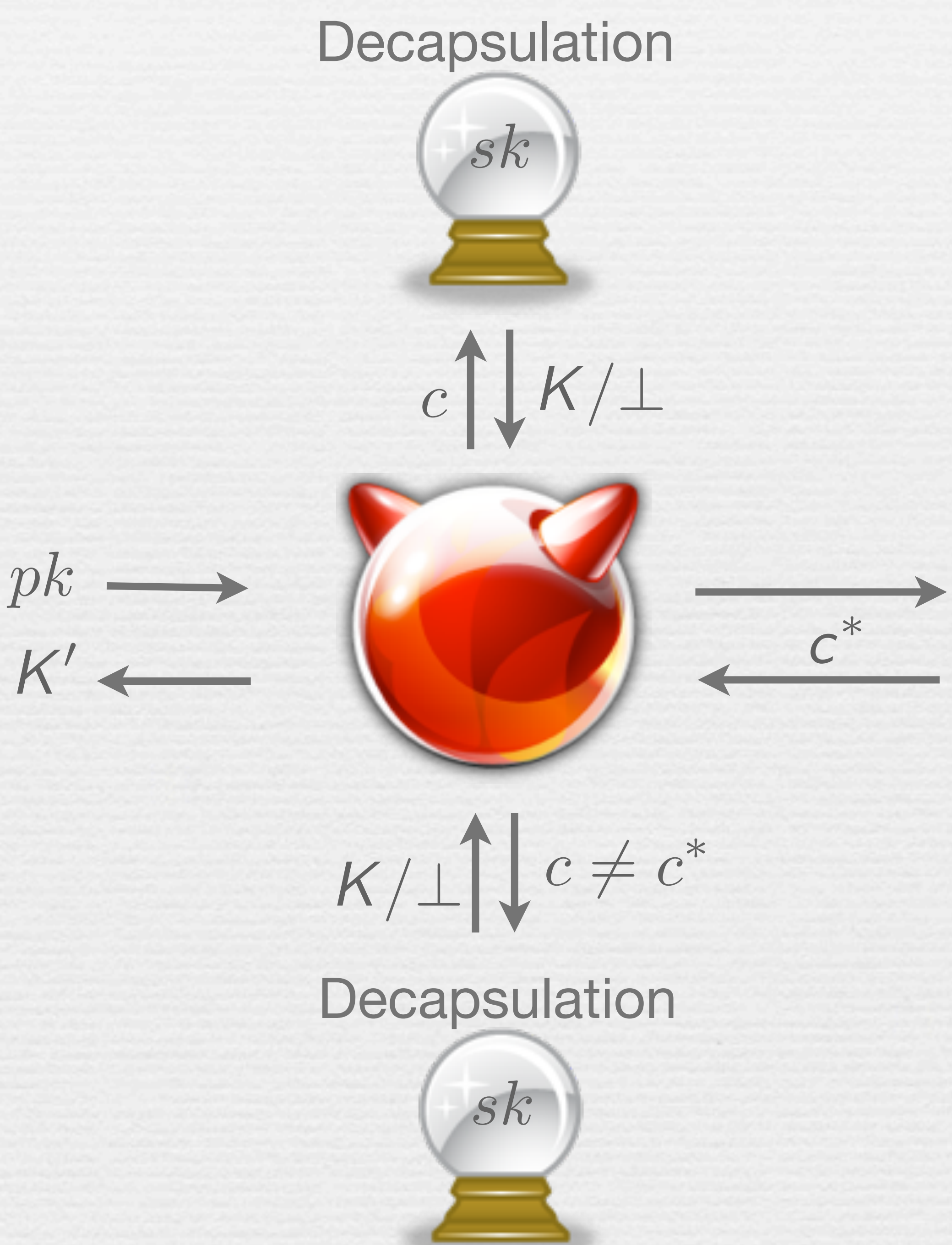
  1. Public key: $pk = (X_1, \dots, X_n, aux) \in \mathbb{G}^n \times \{0,1\}^*$ $\qquad (y_i = \log_g X_i)$

  2. Encapsulation: $C = (c, d) = (g^r, \tilde{f}(pk, r)) \in \mathbb{G} \times \{0,1\}^*$
     $$K = g^{f_0(pk,r)} \prod_{i=1}^{n} X_i^{f_i(pk,r)}$$

  3. Decapsulated key: $K = g^{\psi_0(pk,C,y_1,\dots,y_n)} c^{\psi_1(pk,C,y_1,\dots,y_n)}$
     where $\psi_i(pk, C, y_1, \dots, y_n) = \psi_{i,1}(pk, C) \cdot y_1 + \dots + \psi_{i,n}(pk, C) \cdot y_n$

  4. $\exists \psi_2$ s.t. $d = \psi_2(pk, c, y_1, \dots, y_n)$

OW-CCA Security for KEMs



$(c^*, K^*) \leftarrow \mathsf{Enc}(pk)$

$$\boxed{\mathsf{Adv}^{\text{OW-CCA}}(\ ) = \Pr[K' = K^*]}$$

Non-interactive Problems

- A non-interactive problem in a group is given by

$$\Lambda = (g, p, \mathbb{G}) \longrightarrow \boxed{\mathsf{I}} \longrightarrow (y, w)$$

$$(x, y, w) \longrightarrow \boxed{\mathsf{V}} \longrightarrow \top / \bot$$

$$y \longrightarrow \boxed{\mathsf{U}} \longrightarrow x$$

- Hardness of a non-interactive problem

PPTA

$y \longrightarrow$  $\longrightarrow x$

 wins if $\mathsf{V}(x, y, w) = \top$

$\mathsf{Adv}_P^{\mathsf{NIP}}($$) = \Pr[$  wins$] - \Pr[\mathsf{U}$ wins$]$

P is *hard* if $\mathsf{Adv}_P^{\mathsf{NIP}}($$) < \mathsf{neg}(\lambda) \quad \forall$ 

Non-interactive Problems

- A non-interactive problem in a group is given by

$$\Lambda = (g, p, \mathbb{G}) \longrightarrow \boxed{\mathsf{I}} \longrightarrow (y, w)$$

$$(x, y, w) \longrightarrow \boxed{\mathsf{V}} \longrightarrow \top/\bot$$

$$y \longrightarrow \boxed{\mathsf{U}} \longrightarrow x$$

- Hardness of a non-interactive problem

PPTA

$y \longrightarrow$

wins if $\mathsf{V}(x, y, w) = \top$

$- \Pr[\mathsf{U} \text{ wins}]$

$\mathsf{neg}(\lambda) \quad \forall$

Captured problems:
DDH, CDH, q-SDH, q-ABDHE, IND-CPA, ...

Black-box Reductions

- There is a black-box reduction from the OW-CCA security of a KEM Γ to a non-interactive problem *P* if

Oracle PPTA

$\exists$ 

Any

$\forall$ 

$\mathsf{Adv}_{\Gamma}^{\text{OW-CCA}}($  $) > \mathrm{neg}(\lambda)$

$$\Downarrow$$

$\mathsf{Adv}_{P}^{\text{NIP}}($  $) > \mathrm{neg}(\lambda)$

- This is a fully black-box reduction in the terminology by Reingold et al. [RTV04]

Algebraic Algorithms

- Defined via the existence of an extractor

$(X_1, \dots, X_n; r)$

$\downarrow$

$\downarrow$

Y

$\exists$

$(X_1, \dots, X_n; r)$

$\downarrow$

$\downarrow$

$(y_1, \dots, y_n)$

such that $\prod_{i=1}^{n} X_i^{y_i} = Y$

- The security reductions of existing KEMs defined in prime order groups are all algebraic.

Main Theorem

RISEC

Theorem

$\forall \Gamma \in \mathcal{K} \quad \forall P \in NIP$

$$P \text{ is hard} \quad \Rightarrow \quad \text{OW-CCA}_\Gamma \overset{Alg\ +\ BB}{\not\longrightarrow} P$$

Oracle Separation Lemma

Assume there exists an oracle distribution  such that

Alg PPTA

$\forall \Gamma \in \mathcal{K}$ $\exists$  s.t.  $\leftarrow$  $\mathbf{E}\left[\mathrm{Adv}_{\Gamma}^{\text{OW-CCA}}(\right.$  $\left.)\right] > \mathrm{neg}$

and

Alg PPTA *PPTA* *PPTA*

$\forall P \in NIP$ $\forall$  $\exists$   s.t.  $\leftarrow$ 

$\mathbf{E}\left[\mathrm{Adv}_{P}^{\text{NIP}}(\right.$  $\left.)\right] < \mathrm{Adv}_{P}^{\text{NIP}}($  $) + \mathrm{Adv}^{\text{DL}}($  $)$

Alg + BB

Then, $\forall \Gamma \in \mathcal{K}$ and $\forall P \in NIP$, if P hard: $\quad$ $\textit{OW-CCA}_{\Gamma}$ $\longrightarrow$  P

Additional Observations

Additional Observations

- Looking at the details of the proofs yields a few additional insights
  - The KEM attacker constructed in the proof only requires *n* decryption queries for a KEM with *n* group elements in the public key

Corollary

$\forall \Gamma \in \mathcal{K} \quad \forall P \in NIP$

$$\begin{array}{c} P \text{ is hard} \\ + \\ pk \in \{0,1\}^* \times \mathbb{G}^n \end{array} \quad \Rightarrow \quad \text{OW-}n\text{-CCA}_\Gamma \not\xrightarrow{\text{BB + Alg}} P$$

Additional Observations

- Looking at the details of the proofs yields a few additional insights
  - The KEM attacker constructed in the proof only requires *n* decryption queries for a KEM with *n* group elements in the public key
  - Adaptive decryption queries are not required -- one parallel query is sufficient

Corollary

Corollary

$\forall \Gamma \in \mathcal{K} \quad \forall P \in NIP$

$$P \text{ is hard} \quad \Rightarrow \quad \text{NM-CPA}_{\Gamma} \ \cancel{\xrightarrow{BB + Alg}} \ P$$

Programmable Hash Functions

Programmable Hash Functions

- Programmable hash functions
  - Introduced by Hofheinz and Kiltz [HK08]
  - Provides programmability in the standard model
  - Main application: short signatures

Programmable Hash Functions

- Programmable hash functions
  - Introduced by Hofheinz and Kiltz [HK08]
  - Provides programmability in the standard model
  - Main application: short signatures

- Based on an algebraic (*poly, 1*)-programmable hash function, we can construct a KEM which
  - Is IND-CCA secure based on the DDH problem
  - Has an algebraic black-box security reduction
  - Has a ciphertext overhead of a single group element

Programmable Hash Functions

- Programmable hash functions
  - Introduced by Hofheinz and Kiltz [HK08]
  - Provides programmability in the standard model
  - Main application: short signatures
- Based on an algebraic (*poly, 1*)-programmable hash function, we can construct a KEM
  - Is IND-CCA se
  - Has an algebr
  - Has a ciphert

Corollary
$\forall k \in \mathbb{N}$ there exists no algebraic (poly,k)-programmable hash function in prime order groups

Programmable Hash Functions

- Programmable hash functions
  - Introduced by Hofheinz and Kiltz [HK08]
  - Provides programmability in the standard model
  - Main application: short signatures

- Based on an algebraic (*poly, 1*)-programmable hash function, we can construct a KEM
  - Is IND-CC
  - Has an alg
  - Has a ciph

Corollary

Corollary

$\forall n, k \in \mathbb{N}$ *there exists no algebraic (n,k)-programmable hash function with* $\kappa \in \{0,1\}^* \times \mathbb{G}^m$ $m \leq n$ *in prime order groups*

Summary

- We have shown that
  - There exists no algebraic black-box reduction from the OW-CCA security of a class of efficient KEMs to a non-interactive problem
  - Certain types of programmable hash functions cannot be constructed in prime order groups
- Open problems
  - (Im)possible to construct an IND-CCA secure KEM without pairings based on a non-interactive assumption and with two group element encapsulations?
  - Possible to extend results to constrained CCA security?
  - Possible to make any conclusions about schemes relying on key derivation functions?

Thank you!