SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Chameleon All-But-One Extractable Hash Proof and Its Applications

Gang HAN[1], Hui LI[1], Baodong QIN[2,3*] & Dong ZHENG[2,4]

[1]*School of Electronics and Information, Northwestern Polytechnical University, Xi'an* 710129*, P.R. China;*
[2]*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an* 710121*, P.R. China;*
[3]*State Key Laboratory of Cryptology , P.O.Box5159, Beijing* 100878*, P.R. China;*
[4]*Westone Cryptologic Research Center, Beijing* 100070*, P.R. China*

Appendix A Proof of Theorem 1

Proof. We prove the CCA-security of $\mathcal{PKE}$ using the sequence-of-games approach proposed by Shoup [9]. First, we describe a sequence of games, $\mathbf{Game_i}$ $(0 \leqslant i \leqslant 5)$, where $\mathbf{Game_0}$ is the original IND-CCA game with respect to an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$. Let $\Pr[\text{Success}_i]$ be the success probability of $\mathcal{A}$ in $\mathbf{Game_i}$. Then we show that $\Pr[\text{Success}_i]$ is negligibly close to $\Pr[\text{Success}_{i+1}]$ for all $i = 0, \ldots, 4$. Finally, we show that $\mathcal{A}$ has no advantage in $\mathbf{Game_5}$, i.e. $\Pr[\text{Success}_5] = 1/2$. From this, it follows that $|\Pr[\text{Success}_0] - 1/2|$ is negligible. Hence, the public-key encryption scheme is CCA-seucre. By $c^* = (c_0^*, u^*, \tau^*, b^*)$, we denote the challenge ciphertext. Now, we describe the definitions of $\mathbf{Game_i}$.

$\mathbf{Game_1}$. This game is the same as $\mathbf{Game_0}$ except for a modification to the decryption oracle. When the adversary queries the decryption oracle with a ciphertext $c = (c_0, u, \tau, b)$ $(c \neq c^*)$, the challenger first computes $a = \text{CR}(c_0||u)$, then checks whether $(a, b) = (a^*, b^*)$. If so, it outputs $\perp$, otherwise it outputs what the decryption oracle outputs in $\mathbf{Game_0}$.

$\mathbf{Game_2}$. This game is the same as $\mathbf{Game_1}$ except for the following modifications to the IND-CCA experiment. We replace $\text{EHP.SetupExt}_{\text{ch}}(\text{PP})$ with $\text{EHP.SetupABO}_{\text{ch}}(\text{PP})$ to generate (PK, SK^*) together with a kernel tag space $\mathcal{S}$. In addition, we replace the decryption oracle of $\mathbf{Game_1}$ with a new one that is defined as follows.

> When the adversary queries the decryption oracle with a ciphertext $c = (c_0, u, \tau, b)$, the challenger first computes $a = \text{CR}(c_0||u)$; then
>
> - if $(a, b) = (a^*, b^*)$ or $(a, b) \in \mathcal{S}$, it outputs $\perp$;
> - if $(a, b) \neq (a^*, b^*)$ and $(a, b) \notin \mathcal{S}$, it computes
>
> $$s = \text{EHP.Ext}_{\text{ch}}^*(\text{SK}^*, (a, b), u, \tau);$$
>
> If $(u, s) \in \text{R}_{\text{PP}}$, it outputs $m = c_0 \oplus \text{G}_{\text{PP}}(s)$, else outputs $\perp$.

$\mathbf{Game_3}$. This game is the same as $\mathbf{Game_2}$ except for a modification to the way of computing the challenge ciphertext $c^* = (c_0^*, u^*, \tau^*, b^*)$. When the adversary queries a challenge ciphertext for two messages m_0 and m_1, the challenger samples $(u^*, s^*) \leftarrow \text{SampR}(r^*)$; then computes

$$c_0^* = m_\beta \oplus \text{G}_{\text{PP}}(s^*) \text{ and } \tau^* = \text{EHP.Pub}_{\text{ch}}(\text{PK}, (a^*, b^*), r^*),$$

where $\beta \leftarrow_R \{0, 1\}$, $a^* = \text{CR}(c_0^*||u^*)$ and $b^* = \text{EHP.CompKT}_{\text{ch}}(\text{SK}^*, a^*)$. Finally, it outputs the challenge ciphertext $c^* = (c_0^*, u^*, \tau^*, b^*)$.

$\mathbf{Game_4}$. This game is the same as $\mathbf{Game_3}$ except for a small modification to the way of computing the challenge ciphertext $c^* = (c_0^*, u^*, \tau^*, b^*)$. The challenger uses $\text{EHP.Priv}_{\text{ch}}$ instead of the public evaluation $\text{EHP.Pub}_{\text{ch}}$ to compute $\text{H}_{\text{PK}}((a^*, b^*), u^*)$, that is

$$\tau^* = \text{EHP.Priv}_{\text{ch}}(\text{SK}^*, (a^*, b^*), u^*).$$

* Corresponding author (email: qinbaodong@xupt.edu.cn)

Game$_5$. This game is the same as **Game$_4$** except for a small modification to the challenge ciphertext $c^* = (c_0^*, u^*, \tau^*, b^*)$. The challenger chooses a random K^* from $\{0,1\}^k$ instead of using $\mathrm{G}_{\mathrm{PP}}(s^*)$ to compute c_0^*, that is $c_0^* = m_\beta \oplus K^*$.

Corollary 1. $|\Pr[\mathrm{Success}_0] - \Pr[\mathrm{Success}_1]|$ is negligible, assuming the collision-resistant property of hash function CR.

Proof. Let E be the event that the adversary $\mathcal{A}$ makes a legal (i.e, not equal to c^*) decryption query of the form $c = (c_0, u, \tau, b = b^*)$, where $\mathrm{CR}(c_0||u) = a^*$. We observe that $Game_0$ and $Game_1$ proceed identically until event E occurs. So, we have

$$|\Pr[\mathrm{Success}_0] - \Pr[\mathrm{Success}_1]| \leqslant \Pr[E].$$

Next, we show that event E occurs with negligible probability. Since $\tau = \mathrm{H}_{\mathrm{PK}}(\cdot)$ is determined by its inputs TAG and u, if $c \neq c^*$, we must have $(c_0, u, b) \neq (c_0^*, u^*, b^*)$. So, if event E occurs, we have $(c_0, u) \neq (c_0^*, u^*)$ and $\mathrm{CR}(c_0||u) = \mathrm{CR}(c_0^*||u^*) = a^*$. That is, we break the collision resistance of CR.

Because the hash function CR is collision resistant, we conclude that event E occurs with negligible probability, as desired.

Corollary 2. $|\Pr[\mathrm{Success}_1] - \Pr[\mathrm{Success}_2]|$ is negligible, assuming the statistical indistinguishability of the two public keys respectively generated by $\mathrm{EHP.SetupExt}_{\mathrm{ch}}$ and $\mathrm{EHP.SetupABO}_{\mathrm{ch}}$ and the hardness of finding a kernel tag.

Proof. Let F be the events that in $Game_2$ the adversary $\mathcal{A}$ makes a legal decryption query of the form $c = (c_0, u, \tau, b)$, where $(a = \mathrm{CR}(c_0||u), b) \in \mathcal{S}$.

Next, we show that $Game_1$ and $Game_2$ proceed identically until event F occurs. Since the two public keys respectively generated by $\mathrm{EHP.SetupExt}_{\mathrm{ch}}$ and $\mathrm{EHP.SetupABO}_{\mathrm{ch}}$ are statistically indistinguishable, we have that the adversary's views of (PK, c^*) in $Game_1$ and $Game_2$ are statistically indistinguishable. In addition, for all $(\mathrm{PK}, c = (c_0, u, \tau, b))$, when $(a = \mathrm{CR}(c_0||u), b) \notin \mathcal{S}$, by the definition of the decryption oracle in $Game_2$ and the correctness of all-but-one mode, we have that the adversary's views of $(\mathrm{PK}, \mathcal{D}(c))$ in $Game_1$ and $Game_2$ are also statistically indistinguishable. Thus, we have

$$|\Pr[\mathrm{Success}_1] - \Pr[\mathrm{Success}_2]| \leqslant \Pr[F].$$

Next, we show that event F occurs with negligible probability. Given an adversary $\mathcal{A}$ that can make a legal decryption query of the form $c = (c_0, u, \tau, b)$ such that $(a = \mathrm{CR}(c_0||u), b) \in \mathcal{S}$ with non-negligible probability in $Game_2$, we construct an adversary $\mathcal{B}$ which breaks the hardness of finding a kernel tag of a chameleon ABO-EHP using $\mathcal{A}$ as a subroutine.

On input PK generated by $(\mathrm{PK}, \mathrm{SK}^*, \mathcal{S}) \leftarrow \mathrm{EHP.SetupABO}_{\mathrm{ch}}(\mathrm{PP})$, $\mathcal{B}$ chooses a collision-resistant hash function CR, and gives $pk = (\mathrm{PP}, \mathrm{PK}, \mathrm{CR})$ to $\mathcal{A}$. When $\mathcal{A}$ makes a decryption query $c = (c_0, u, \tau, b)$, $\mathcal{B}$ queries its extraction oracle with (TAG, u, τ), where $\mathrm{TAG} = (\mathrm{CR}(c_0||u), b)$ and is given in return $s = \mathcal{O}_{\mathrm{Ext}}(\cdot)$. If s is the special symbol $\perp$, $\mathcal{B}$ outputs it directly. Otherwise, s should be equal to $\mathrm{EHP.Ext}_{\mathrm{ch}}^*(\mathrm{SK}^*, \mathrm{TAG}, u, \tau)$ and $(u, s) \in \mathrm{R}_{\mathrm{PP}}$. $\mathcal{B}$ outputs $\mathrm{G}_{\mathrm{PP}}(s) \oplus c_0$.

When $\mathcal{A}$ asks to be challenged on two messages $m_0, m_1 \in \{0,1\}^k$, $\mathcal{B}$ creates the challenge ciphertext $c^* = (c_0^*, u^*, \tau^*, b^*)$ by running $\mathcal{E}(pk, m_\beta)$, where $\beta \xleftarrow{\$} \{0,1\}$. When $\mathcal{A}$ continues to make a decryption query $c = (c_0, u, \tau, b)$, $\mathcal{B}$ first checks whether $(\mathrm{CR}(c_0||u), b) = (\mathrm{CR}(c_0^*||u^*), b^*)$. If so, $\mathcal{B}$ outputs $\perp$. Otherwise $\mathcal{B}$ handles it as before. Finally, $\mathcal{A}$ outputs a bit β'. Let $H = \{\mathrm{TAG}_i\}$ be the set of tags where $\mathcal{B}$ queries $\mathcal{O}_{\mathrm{Ext}}(\cdot)$ with (TAG, u, τ). Now, $\mathcal{B}$ uniformly chooses a tag from H as its final output.

It is clear by construction that $\mathcal{B}$ perfectly simulates $Game_2$ to $\mathcal{A}$. Thus, $\mathcal{B}$ wins its challenge with probability at least $\frac{\Pr[F]}{|H|}$.

Because $\mathcal{A}$ makes a polynomial number of queries to the extractable oracle and $\mathcal{B}$ has negligible probability to find a kernel tag of a chameleon ABO-EHP, we conclude that event F occurs with negligible probability, as desired.

Corollary 3. $|\Pr[\mathrm{Success}_2] - \Pr[\mathrm{Success}_3]|$ is negligible, assuming the hardness of distinguishing a kernel tag from a non-kernel tag.

Proof. For any PPT adversary $\mathcal{A}$ that can distinguish $Game_3$ from $Game_2$, we describe an efficient distinguisher algorithm $\mathcal{B}$ against the indistinguishability of a kernel tag and a uniformly picked tag of a chameleon ABO-EHP as follows.

On input PK generated by $(\mathrm{PK}, \mathrm{SK}^*, \mathcal{S}) \leftarrow \mathrm{EHP.SetupABO}_{\mathrm{ch}}(\mathrm{PP})$, $\mathcal{B}$ simulates the key generation algorithm $\mathcal{G}$ and decryption oracle $\mathcal{D}$ just as in the proof of Claim 2. When $\mathcal{A}$ asks to be challenged on two messages $m_0, m_1 \in \{0,1\}^k$, $\mathcal{B}$ picks $\beta \xleftarrow{\$} \{0,1\}$ and constructs the challenge ciphertext as follows:

1. It samples $(u^*, s^*) \leftarrow \mathrm{SampR}(r^*)$ and computes

$$c_0^* = m_\beta \oplus \mathrm{G}_{\mathrm{PP}}(s^*), a^* = \mathrm{CR}(c_0^*||u^*).$$

2. Next, it gives a^* to its challenger and gets the response as b^*. Then, it computes $\tau^* = \mathrm{EHP.Pub}_{\mathrm{ch}}(\mathrm{PK}, (a^*, b^*), r^*)$.

3. Finally, it sets the challenge ciphertext as $(c_0^*, u^*, \tau^*, b^*)$.

When $\mathcal{A}$ halts, $\mathcal{B}$ returns its output.

We observe that when $b^* = \mathrm{CompKT}_{\mathrm{ch}}(\mathrm{SK}^*, a^*)$, $\mathcal{B}$ simulates $Game_3$ perfectly, otherwise, it simulates $Game_2$ perfectly. Thus, $\mathcal{B}$ is an efficient distinguisher algorithm. Since EHP has the property of indistinguishability of a kernel tag and a uniformly picked tag for any PPT adversary, this implies that $|\Pr[\mathrm{Success}_2] - \Pr[\mathrm{Success}_3]|$ is negligible.

Corollary 4. $\Pr[\mathrm{Success}_3]$=$\Pr[\mathrm{Success}_4]$.

Proof. It is clear that $Game_3$ and $Game_4$ are identically distributed by correctness of the chameleon all-but-one mode.

Corollary 5. $|\Pr[\mathrm{Success}_4] - \Pr[\mathrm{Success}_5]|$ is negligible, assuming the pseudorandomness of the generator $\mathrm{G}_{\mathrm{PP}}(\cdot)$.

Proof. Observe that in $Game_4$, we never use knowledge of the witness s^* or randomness r^* associated with u^* except in the computation of the first element $c_0^* = m_\beta \oplus K^*$ of the challenge ciphertext $(c_0^*, u^*, \tau^*, b^*)$. This implies that we can construct a PPT simulator algorithm that on input (PP, u^*, K^*), simulates $Game_4$ perfectly if $K^* = \text{G}_{\text{PP}}(s^*)$ (recall here that $(u^*, s^*) \leftarrow \text{SampR}(r^*)$) and that simulates $Game_5$ perfectly if K^* is randomly chosen from $\{0,1\}^k$. By the pseudorandomness of $\text{G}_{\text{PP}}(\cdot)$, the claim follows.

Corollary 6. $\Pr[\text{Success}_5] = \frac{1}{2}$.

Proof. Observe that in this game, the challenge ciphertext c^* is independent of the adversary's challenge messages m_0 and m_1. So, the adversary's success probability is exactly 1/2.

Combining Corollary 1 to Corollary 6, we obtain Theorem 1.

Appendix B Proof of Theorem 2 and Instantiations

Proof. We show that the construction in Theorem 2 satisfies the required properties of chameleon ABO-EHP system.

(*Correctness*) The correctness of the algorithms in the above extractable hash proof system can be checked directly.

(*Hardness*) For any PPT adversary, it is hard to find a tag $(a, b) \in \mathcal{S}$. Observe that x_a and x_b are initially hidden by blinding factors β_1^* and β_2^* respectively and the public key PK does not leak any information about either x_a or x_b. Thus, for any tag $(a, b) \in \mathbb{Z}_q \times \mathbb{Z}_q$, there are exactly q possible values of $a + b \cdot x_a + x_b$ from the view point of an adversary. An adversary that has access to the extractable oracle $\mathcal{O}_{\text{Ext}}(\cdot)$, can discover whether $(a, b) \in \mathcal{S}$ (i.e. $a + b \cdot x_a + x_b = 0 \bmod q$). Information-theoretically, for the adversary's $(i+1)$st access to $\mathcal{O}_{\text{Ext}}(\cdot)$, the probability that $a + b \cdot x_a + x_b = 0$ is at most $1/(q - i)$. Thus, for a PPT adversary that makes $p(\lambda)$ queries to $\mathcal{O}_{\text{Ext}}(\cdot)$, his success probability of finding a kernel tag is at most

$$1 - \prod_{i=1}^{p(\lambda)} (1 - \frac{1}{q - i + 1})$$

which is negligible in λ.

(*Indistinguishability I*) It is clear that the two public keys respectively generated in the extractable mode and in the all-but-one mode have the same distributions. So, they are statistically indistinguishable.

(*Indistinguishability II*) For any $s, t \in \mathbb{Z}_q$ and any $(a, b_0), (a, b_1) \in \mathbb{Z}_q \times \mathbb{Z}_q$ $(b_0 \neq b_1)$, it always has x_a and x_b such that

$$\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} b_0 & 1 \\ b_1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_a \\ x_b \end{pmatrix} + \begin{pmatrix} a \\ a \end{pmatrix}.$$

Thus, all the tags are equally likely in the view of the adversary. Since the adversary only makes a polynomial number of queries to the extractable oracle, we have that the adversary has negligible probability to distinguish a random tag in $\mathcal{S}$ from a random tag in $\mathcal{T}$.

Applying the chameleon ABO-EHP systems for (twin) Diffie-Hellman relations with suitable pseudorandom generators, we can derive the following PKE schemes as described in Fig. B1, Fig. B2 and Fig. B3.

$\mathcal{G}(1^\lambda)$:	$\mathcal{E}(pk, m)$:	$\mathcal{D}(sk, c)$:
$\text{PP} := (g, g^\alpha, g^\gamma)$	$u := g^r$, $r \xleftarrow{\$} \mathbb{Z}_p$	parse c as (c_0, u, τ, b)
$(x_1, x_2) \xleftarrow{\$} \mathbb{Z}_q^2$	$c_0 := m \oplus e(g^\alpha, g^\gamma)^r$	$a := \text{CR}(c_0 \| u)$, check
$(X_1, X_2) := (g^{x_1}, g^{x_2})$	$a := \text{CR}(c_0 \| u)$, $b \xleftarrow{\$} \mathbb{Z}_q$	$e(g, \tau) = e(u, g^{\alpha a} X_1^b X_2)$
$pk := (\text{PP}, X_1, X_2)$	$\tau := (g^{\alpha a} X_1^b X_2)^r$	$s := (\tau u^{-bx_1 - x_2})^{a^{-1}}$
$sk := (pk, x_1, x_2)$	$c := (c_0, u, \tau, b)$	$m := c_0 \oplus e(s, g^\gamma)$
return (pk, sk)	return c	return m

Figure B1 A CCA-secure PKE Scheme under the DBDH Assumption

The description of the scheme in Fig. B1 can be improved as follows. We can check the consistency of a ciphertext via $\tau = u^{a\alpha + bx_1 + x_2}$ and then decrypt it directly via $m := c_0 \oplus e(u, g^{\alpha\gamma})$ if we regard α and $g^{\alpha\gamma}$ as secret key parts. In the encryption operation, we can avoid computing the pairing by setting $e(g^\alpha, g^\gamma)$ as a public key. As a result, we obtain exactly the scheme of [7]. That is, our generic construction encompasses the scheme of [7].

Appendix C Comparison

To demonstrate the practicality of our generic approach for constructing CCA-secure PKE schemes, we compare the efficiency of the concrete schemes derived from our approach with previous related schemes.

Table C1 is an efficiency comparison among some DBDH-based PKE schemes with CCA-security in the standard model. In Table C1, l_g and l_{g_T} denote the length of the representation of an element in G and G_T respectively, and l_q denotes the length of the representation of an element in $\mathbb{Z}_q$. "vk" and "sig" respectively denote the public key and signature of the

$\mathcal{G}(1^\lambda)$:	$\mathcal{E}(pk, m)$:	$\mathcal{D}(sk, c)$:
$\text{PP} := (g, g^{\alpha_1}, g^{\alpha_2}, R)$	for $i = 1$ to ℓ	parse c as
$(x_1, x_2, x_3, x_4) \xleftarrow{\$} \mathbb{Z}_q^4$	$u_i := g^{r_i}$, $r_i \xleftarrow{\$} \mathbb{Z}_q$	$(c_0, (u_i, \tau_{i1}, \tau_{i2})_{i=1}^{\ell}, b)$
$(X_1, X_2) := (g^{x_1}, g^{x_2})$	$K := (\text{GL}_R(g^{\alpha_1 r_i}))_{i=1}^{\ell}$	$a := \text{CR}(c_0 \|\| (u_i)_{i=1}^{\ell})$
$(X_3, X_4) := (g^{x_3}, g^{x_4})$	$c_0 := m \oplus K$, $b \xleftarrow{\$} \mathbb{Z}_q$	for $i = 1$ to ℓ, check
$pk := (\text{PP}, X_1, X_2, X_3, X_4)$	$a := \text{CR}(c_0 \|\| (u_i)_{i=1}^{\ell})$	$\tau_{i1} := u_i^{a\alpha_1 + bx_1 + x_2}$
$sk := (pk, x_1, x_2, x_3, x_4)$	for $i = 1, \ldots, \ell$	$\tau_{i2} := u_i^{a\alpha_2 + bx_3 + x_4}$
return (pk, sk)	$\tau_{i1} := (g^{\alpha_1 a} X_1^b X_2)^{r_i}$	$s_i := (\tau_{i1} u_i^{-bx_1 - x_2})^{a^{-1}}$
	$\tau_{i2} := (g^{\alpha_2 a} X_3^b X_4)^{r_i}$	$K := (\text{GL}_R(s_i))_{i=1}^{\ell}$
	$c := (c_0, (u_i, \tau_{i1}, \tau_{i2})_{i=1}^{\ell}, b)$	$m := c_0 \oplus K$
	return c	return m

Figure B2 A CCA-secure PKE Scheme under the CDH Assumption

$\mathcal{G}(1^\lambda)$:	$\mathcal{E}(pk, m)$:	$\mathcal{D}(sk, c)$:
for $i = 1$ to 6	$u := g^r$, $r \xleftarrow{\$} \mathbb{Z}_q$	parse c as $(c_0, u, \tau_1, \tau_2, b)$
$X_i := g^{x_i}$, $x_i \xleftarrow{\$} \mathbb{Z}_q$	$K := (\text{GL}_R(Z_i^r))_{i=1}^{\ell}$	$a := \text{CR}(c_0 \|\| u)$, check
for $i = 1$ to ℓ	$c_0 := m \oplus K$	$\tau_1 := u^{ax_1 + bx_2 + x_3}$
$Z_i := g^{z_i}$, $z_i \xleftarrow{\$} \mathbb{Z}_q$	$a := \text{CR}(c_0 \|\| u)$, $b \xleftarrow{\$} \mathbb{Z}_q$	$\tau_2 := u^{ax_4 + bx_5 + x_6}$
$pk := (g, R, (X_i)_{i=1}^6, (Z_i)_{i=1}^{\ell})$	$\tau_1 := (X_1^a X_2^b X_3)^r$	for $i = 1$ to ℓ, $Z_i := u^{z_i}$
$sk := (pk, (x_i)_{i=1}^6, (z_i)_{i=1}^{\ell})$	$\tau_2 := (X_4^a X_5^b X_6)^r$	$K := (\text{GL}_R(Z_i))_{i=1}^{\ell}$
return (pk, sk)	$c := (c_0, u, \tau_1, \tau_2, b)$	$m := c_0 \oplus K$
	return c	return m

Figure B3 A variant of CDH-base PKE Scheme with Constant Size Ciphertext

signature scheme. Let "mac" be the message authentication code. "#Sig" and "#Vrfy" respectively denote the number of operations required for signature generation and signature verification. "exp" denotes an exponentiation operation (and some of the exponentiations are actually fixed-base multi-exponentiations, e.g., the computation of $\tau := (g^{\alpha a} X_1^b X_2)^r$ in Fig. B1 is viewed as one fixed-base multiplication exponentiation with fixed base (g^α, X_1, X_2)). "pr" denotes a pairing operation. We ignore all other operations. Note that, our approach encompasses the CCA-secure PKE schemes derived from the identity-based techniques in [7]. By the comparison from Table C1, it shows that our scheme obtained by chameleon EHP system has small public key size and also has efficient encryption and decryption.

Table C2 is an efficiency comparison among some CDH based PKE schemes with CCA-security in the standard model. In Table C2, l_g and l_q denote the length of the representation of an element in G and $\mathbb{Z}_q$ respectively. l_m and l_t respectively denote the length of message and message authentication code. "exp" denotes an exponentiation operation. We ignore all other operations. Let $l'_m = \min\{l_m, \lambda_s\}$ (λ_s is the PRG seed size) and $n = l'_m + l_t$. For concreteness, we consider a security parameter of 80 bits for both PRG and MAC, i.e. $l_t = \lambda_s = 80$ (Usually, this is the minimum requirement, otherwise, PRG and MAC may suffer from brute force attacks), and a group with $l_q = 160$ bits prime order. In addition, we assume that a PIN number consists of six decimal digital. In this case, we can use at most 20 bits to represent a PIN number. Taking the values of $l_q = 160$, $l_t = 80$, $l'_m = l_m = 20$ and $n = 100$ into Table C2, we roughly obtain a concrete efficiency comparison in Table C3.

Table C3 shows that our schemes require significantly fewer exponentiations in both encryption and decryption than the scheme of [11] obtained from normal extractable hash proof systems following hybrid encryption paradigm. Compared with other schemes, ours in Fig. B3 also has improved efficiency in terms of encryption and decryption for short messages.

Table C1 Efficiency comparison among some DBDH-based PKE schemes.

Schemes	Public-Key Size	Ciphertext Overhead	Encryption [#pr, #exp,	Decryption #Sig, #Vrfy]
CHK [3]	$4l_g + l_{g_T}$	$2l_g + \|\text{vk}\| + \|\text{sig}\|$	[0, 3, 1, 0]	[1, 1, 0, 1]
BK [1]	$4l_g + l_{g_T}$	$2l_g + \|\text{mac}\|$	[0, 3, 0, 0]	[1, 1, 0, 0]
BMW [2]	$162l_g + l_{g_T}$	$2l_g$	[0, 4, 0, 0]	[1, 1, 0, 0]
KTL [6]	$163l_g + l_{g_T}$	$2l_g$	[0, 4, 0, 0]	[1, 1, 0, 0]
Tan [10]	$6l_g + l_{g_T}$	$3l_g$	[0, 4, 0, 0]	[1, 2, 0, 0]
LDLK [7]	$4l_g + l_{g_T}$	$2l_g + l_q$	[0, 3, 0, 0]	[1, 1, 0, 0]
Fig. B1	$4l_g + l_{g_T}$	$2l_g + l_q$	[0, 3, 0, 0]	[1, 1, 0, 0]

Table C2 Efficiency comparison among some CDH-based PKE schemes.

Schemes	Public-Key Size	Ciphertext Overhead	Encryption #exp	Decryption #exp
CKS [4]	$2(n+1)l_g$	$(n+2)l_g + l_t$	$3n+1$	$2n+1$
HJKS [5]	$(n+4)l_g$	$3l_g + l_t$	$n+5$	$n+2$
Wee [11]	$4l_g$	$3nl_g + l_t$	$6n$	$3n$
Fig. B2	$6l_g$	$(3l'_m+1)l_g + l_q$	$8l'_m$	$3l'_m$
Fig. B3	$(l'_m+6)l_g$	$3l_g + l_q$	l'_m+7	l'_m+2

Table C3 An example of Table C2 with security level $\lambda = 80$ and message length $l_m = 20$.

Schemes	Public-Key Size	Ciphertext Overhead	Encryption #exp	Decryption #exp
CKS [4]	$201l_g$	$102l_g + 80$	301	201
HJKS [5]	$104l_g$	$3l_g + 80$	105	102
Wee [11]	$4l_g$	$300l_g + 80$	600	300
Fig. B2	$6l_g$	$61l_g + 160$	160	60
Fig. B3	$26l_g$	$3l_g + 160$	27	22

References

1 Boneh D, Katz J. Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In: Proceedings of the Cryptographers' Track at the RSA Conference (CT-RSA 2005), San Francisco, 2005. 87–103

2 Boyen X, Mei Q X, Waters B. Direct chosen ciphertext security from identity-based techniques. In: Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS 2005), Alexandria, 2005. 320–329

3 Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Advances in Cryptology - EUROCRYPT 2004, Interlaken, 2004. 207–222

4 Cash D, Kiltz E, Shoup V. The twin Diffie-Hellman problem and applications. J. Cryptology, 2009, 22(4): 470–504

5 Haralambiev K, Jager T, Kiltz E, Shoup V. Simple and efficient public-key encryption from computational Diffie-Hellman in the standard model. In: Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2013), Paris, 2010. 1–18

6 Kang L, Tang X H, Liu J F. Tight chosen ciphertext attack (CCA)-secure hybrid encryption scheme with full public verifiability. SCIENCE CHINA Information Sciences, 2014, 57(11): 1–14

7 Lai J Z, Deng R H, Liu S L, Kou W D. Efficient CCA-secure PKE from identity-based techniques. In: Proceedings of the Cryptographers' Track at the RSA Conference (CT-RSA 2010), San Francisco, 2010. 132–147

8 Liu Y M, Li B, Lu X H, Jia D D. Efficient CCA-secure CDH based KEM balanced between ciphertext and key. In: Proceedings of the 16th Australasian Conference on Information Security and Privacy (ACISP 2011), Melbourne, 2011. 310–318

9 Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. IACR Cryptology ePrint Archive 2004, 332 (2004), http://eprint.iacr.org/2004/332

10 Tan, C.H.: Secure public-key encryption scheme without random oracles. Inf. Sci., 2008, 178(17): 3435–3442

11 Wee H. Efficient chosen-ciphertext security via extractable hash proofs. In: Advances in Cryptology - CRYPTO 2010, Santa Barbara, 2010. 314–332