SCIENCE CHINA
Information Sciences

• LETTER •

September 2018, Vol. 61 099103:1–099103:3
https://doi.org/10.1007/s11432-017-9369-9

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*, China;*
[2]*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an* 710121*, China;*
[3]*State Key Laboratory of Cryptology, P.O. Box* 5159*, Beijing* 100878*, China;*
[4]*Westone Cryptologic Research Center, Beijing* 100070*, China*

Received 16 November 2017/Accepted 31 January 2018/Published online 23 April 2018

Citation Han G, Li H, Qin B D, et al. Chameleon all-but-one extractable hash proof and its applications. Sci China Inf Sci, 2018, 61(9): 099103, https://doi.org/10.1007/s11432-017-9369-9

Dear editor,

We will introduce the notion of chameleon All-But-One Extractable Hash Proof (ABO-EHP) system. It is a special kind of ABO-EHP [1] with a tag space $\mathcal{T}$ that comprises two branches, denoted by $\mathcal{T}_{\mathbb{A}} \times \mathcal{T}_{\mathbb{B}}$. Specifically, the tag space contains a subset $\mathcal{S} \subset \mathcal{T}$ and satisfies the so-called chameleon property. That is, for any $a \in \mathcal{T}_{\mathbb{A}}$, there is a unique and special $b \in \mathcal{T}_{\mathbb{B}}$ (computed via a trapdoor) making $(a, b) \in \mathcal{S}$. The chameleon property allows us to construct public-key encryption (PKE) schemes from chameleon ABO-EHP systems directly, not relying on hybrid encryption mechanism. When encrypting short messages, e.g., a PIN number, the direct construction in some sense is more efficient than the hybrid encryption schemes of [1–3] under the computational Diffie-Hellman (CDH) assumption. In the following, we first give a formal definition of chameleon ABO-EHP system. Then, we show how to construct a chosen-ciphertext secure (CCA) PKE scheme from a chameleon ABO-EHP system. Finally, we present instantiations of chameleon ABO-EHP system for constructing efficient CCA-secure PKE schemes.

Chameleon ABO-EHP system. First, we briefly recall the definition of binary relations that will be used in the chameleon ABO-EHP system.

Definition 1 (Binary relation [1])**.** A fixed family of binary relations R_{PP}, indexed by a public parameter PP, satisfies the following properties.

- (Efficiency) Given a security parameter 1^λ, there is an efficient algorithm SampPP to sample PP, and efficient algorithm SampR to sample R_{PP}. R_{PP} is also efficiently verifiable, possibly via some trapdoor for PP.
- (One-Wayness) Given a random u, it is hard to find s such that $(u, s) \in R_{\text{PP}}$.
- (Pseudorandomness) There is a pseudorandom generator G_{PP} for the relation R_{PP}, such that for any PPT algorithm $\mathcal{A}$, it is hard to distinguish $K_0 \leftarrow G_{\text{PP}}(s)$ from a random $K_1 \overset{\$}{\leftarrow} \{0,1\}^k$, where k is the length of the output from the generator.

By the Goldreich-Levin hard-core bit function GL$(\cdot)$ [4], there always exits a one-bit output generator G_{PP} so long as computing s given u is hard on average. To derive a linear number of hard-core bits, it needs to iterate a one-way permutation or relies on decisional assumptions.

Definition 2 (Chameleon ABO-EHP)**.** Let $\{H_{\text{PK}}\}$ be a family of hash functions. It is indexed by a public key PK and takes additionally a tag (from the tag space $\mathcal{T}_{\mathbb{A}} \times \mathcal{T}_{\mathbb{B}}$) as input. Formally, a chameleon ABO-EHP associated with a one-way relation R_{PP} consists of a tuple of algorithms (SetupExt$_{\text{ch}}$, SetupABO$_{\text{ch}}$, Pub$_{\text{ch}}$, Ext$_{\text{ch}}$,

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

$\mathrm{Ext}^*_{\mathrm{ch}}$, $\mathrm{CompKT}_{\mathrm{ch}}$, $\mathrm{Priv}_{\mathrm{ch}}$) and the following properties hold.

- (Public evaluation) For all $(\textsc{pk}, \textsc{sk})$ generated by $\mathrm{SetupExt}_{\mathrm{ch}}(\textsc{pp})$, all $\textsc{tag} \overset{\$}{\leftarrow} \mathcal{T}_{\mathbb{A}} \times \mathcal{T}_{\mathbb{B}}$ and all $(u, s) \leftarrow \mathrm{SampR}(r)$:

$$\mathrm{Pub}_{\mathrm{ch}}(\textsc{pk}, \textsc{tag}, r) = H_{\textsc{pk}}(\textsc{tag}, u).$$

- (Extraction mode) For all $(\textsc{pk}, \textsc{sk})$ generated by $\mathrm{SetupExt}_{\mathrm{ch}}(\textsc{pp})$, and all $(\textsc{tag}, u, \tau)$:

$$\tau = H_{PK}(\textsc{tag}, u) \Leftrightarrow (u, \mathrm{Ext}_{\mathrm{ch}}(\textsc{sk}, \textsc{tag}, u, \tau)) \in R.$$

- (Chameleon all-but-one mode) For all $(\textsc{pk}, \textsc{sk}^*, \mathcal{S}) \leftarrow \mathrm{SetupABO}_{\mathrm{ch}}(\textsc{pp})$, all $\textsc{tag}^* \in \mathcal{S}$ and all $(u, s) \in R$,

$$\mathrm{Priv}_{\mathrm{ch}}(\textsc{sk}^*, \textsc{tag}^*, u) = H_{\textsc{pk}}(\textsc{tag}^*, u).$$

In addition, for all $\textsc{tag} \in \mathcal{T} \setminus \mathcal{S}$, and all (u, τ):

$$\tau = H_{\textsc{pk}}(\textsc{tag}, u) \Leftrightarrow (u, \mathrm{Ext}^*_{\mathrm{ch}}(\textsc{sk}^*, \textsc{tag}, u, \tau)) \in R.$$

- (Chameleon property) For all $(\textsc{pk}, \textsc{sk}^*, \mathcal{S})$ generated by $\mathrm{SetupABO}_{\mathrm{ch}}(\textsc{pp})$, and all $a \in \mathcal{T}_{\mathbb{A}}$, there is a unique $b \in \mathcal{T}_{\mathbb{B}}$ such that $(a, b) \in \mathcal{S}$. Further, b can be efficiently computed by

$$b = \mathrm{CompKT}_{\mathrm{ch}}(\textsc{sk}^*, a).$$

- (Hardness) We require that it is hard to find a kernel tag for any adversary $\mathcal{A}$ that has adaptive access to the extraction oracle $\mathcal{O}_{\mathrm{Ext}}(\cdot)$; a formal definition of this oracle is given in Definition 3 shortly. Formally, for any PPT adversary $\mathcal{A}$,

$$\Pr\left[(a,b) \in \mathcal{S} : \begin{array}{l} \textsc{pp} \leftarrow \mathrm{SampPP}(1^\lambda); \\ (\textsc{pk}, \textsc{sk}^*, \mathcal{S}) \leftarrow \\ \qquad \mathrm{SetupABO}_{\mathrm{ch}}(\textsc{pp}); \\ (a, b) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{Ext}}(\cdot)}(\textsc{pp}, \textsc{pk}). \end{array}\right]$$

is a negligible function $\mathrm{negl}(\lambda)$.

- (Indistinguishability I) The two public keys (i.e. $\textsc{pk}$) respectively generated by $\mathrm{SetupExt}_{\mathrm{ch}}(\textsc{pp})$ and $\mathrm{SetupABO}_{\mathrm{ch}}(\textsc{tag}^*, \textsc{pp})$ are statistically indistinguishable.

- (Indistinguishability II) For all $(\textsc{pk}, \textsc{sk}^*, \mathcal{S})$ generated by $\mathrm{SetupABO}_{\mathrm{ch}}(\textsc{pp})$ and all $a \in \mathcal{T}_{\mathbb{A}}$, we require that for any adversary that has adaptive access to the extraction oracle $\mathcal{O}_{\mathrm{Ext}}(\cdot)$, it is hard to distinguish a kernel tag (a, b_0), where $b_0 = \mathrm{CompKT}_{\mathrm{ch}}(\textsc{tag}^*, a)$, from (a, b_1), where b_1 is uniformly chosen from $\mathcal{T}_{\mathbb{B}}$. Formally, for any PPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$,

$$\left|\Pr\left[\beta' = \beta : \begin{array}{l} \textsc{pp} \leftarrow \mathrm{SampPP}(1^\lambda); \\ (\textsc{pk}, \textsc{sk}^*, \mathcal{S}) \leftarrow \\ \qquad \mathrm{SetupABO}_{\mathrm{ch}}(\textsc{pp}); \\ a \leftarrow \mathcal{A}_1^{\mathcal{O}_{\mathrm{Ext}}(\cdot)}(\textsc{pp}, \textsc{pk}); \\ b_0 = \mathrm{CompKT}_{\mathrm{ch}}(\textsc{sk}^*, a); \\ b_1 \overset{\$}{\leftarrow} \mathcal{T}_{\mathbb{B}}; \beta \overset{\$}{\leftarrow} \{0,1\}; \\ \beta' \leftarrow \mathcal{A}_2^{\mathcal{O}_{\mathrm{Ext}}(\cdot)}(\textsc{pp}, \textsc{pk}, a, b_\beta). \end{array}\right] - \frac{1}{2}\right|$$

is a negligible function $\mathrm{negl}(\lambda)$, where $\mathcal{A}_2$ is restricted not to ask $(\textsc{tag}, u, \tau)$ such that $\textsc{tag} = (a, b_\beta)$ to the extraction oracle $\mathcal{O}_{\mathrm{Ext}}(\cdot)$.

Definition 3 (Extraction oracle)**.** An extraction oracle $\mathcal{O}_{\mathrm{Ext}}(\cdot)$ is associated with a chameleon ABO-EHP. For all $(\textsc{pk}, \textsc{sk}^*, \mathcal{S})$ generated by $\mathrm{SetupABO}_{\mathrm{ch}}(\textsc{pp})$, where $\mathcal{S} \subset \mathcal{T}$, $\mathcal{O}_{\mathrm{Ext}}(\cdot)$ works as follows:
On input $(\textsc{tag}, u, \tau)$,

- If $\textsc{tag} \in \mathcal{S}$, output a special symbol $\perp$;
- If $\textsc{tag} \in \mathcal{T} \setminus \mathcal{S}$, compute $s = \mathrm{Ext}^*_{\mathrm{ch}}(\textsc{sk}^*, \textsc{tag}, u, \tau)$. If $(u, s) \in R_{\textsc{pp}}$, output s, else output $\perp$.

CCA-secure PKE scheme from chameleon ABO-EHP system. Let $R_{\textsc{pp}}$ be a binary relation indexed by a public parameter $\textsc{pp}$ and let EHP be a chameleon all-but-one hash proof system related to $R_{\textsc{pp}}$. Suppose that $\mathcal{T}_{\mathbb{A}} \times \mathcal{T}_{\mathbb{B}}$ being the tag space and CR: $\{0,1\}^* \to \mathcal{T}_{\mathbb{A}}$ being a collision-resistant hash function.

CCA-secure PKE scheme. Assume the message space is $\{0,1\}^k$, matching with the output space of $\mathrm{G}_{\textsc{pp}}(\cdot)$. Our PKE scheme consists of three PPT algorithm $\mathcal{PKE} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ and is described as follows.

- (Key Generation) $\mathcal{G}(1^\lambda)$: Given a security parameter 1^λ, it runs $\textsc{pp} \leftarrow \mathrm{SampPP}(1^\lambda)$, $(\textsc{pk}, \textsc{sk}) \leftarrow \mathrm{EHP.SetupExt}_{\mathrm{ch}}(\textsc{pp})$ and chooses a collision-resistant hash function CR. Finally, it outputs a public/secret key pair (pk, sk), where $pk = (\textsc{pp}, \textsc{pk}, \mathrm{CR})$ and $sk = \textsc{sk}$.
- (Encryption) $\mathcal{E}(pk, m)$: Given a message $m \in \{0,1\}^k$ and a public key pk, it samples $(u, s) \leftarrow \mathrm{SampR}(r)$ and chooses $b \overset{\$}{\leftarrow} \mathcal{T}_{\mathbb{B}}$. Then, it computes $c_0 = m \oplus G_{\textsc{pp}}(s)$, $a = \mathrm{CR}(c_0 || u)$ and $\tau = \mathrm{EHP.Pub}_{\mathrm{ch}}(\textsc{pk}, (a, b), u)$. Finally, it outputs a ciphertext $c = (c_0, u, \tau, b)$.
- (Decryption) $\mathcal{D}(sk, c)$: Given a ciphertext c and a secret key sk, it parses c as (c_0, u, τ, b). It then computes $a = \mathrm{CR}(c_0 || u)$ and $s = \mathrm{EHP.Ext}_{\mathrm{ch}}(\textsc{sk}, (a, b), u, \tau)$. After that, it checks whether $(u, s) \in R_{\textsc{pp}}$. If not, it outputs $\perp$. Otherwise, it computes and outputs $m = c_0 \oplus G_{\textsc{pp}}(s)$.

To encrypt a message with length $|m| > k$, we can use a pseudorandom generator PRG to extend

$K = \mathrm{G}_{\text{PP}}(s)$ to K' so that $|K'| = |m|$. If K is shorter than the seed length of PRG, we may apply the means proposed in [1] to achieve it.

Theorem 1. If G_{PP} for the binary relation R_{PP} is pseudorandom and CR is a collision-resistant hash function, then $\mathcal{PKE}$ is a CCA-secure PKE scheme.

The proof of Theorem 1 is given in Appendix A.

We now give an example of chameleon ABO-EHP from the Diffie-Hellman (DH) relation. Let $\mathbb{G} = (q, G, g)$ be a description of a cyclic group G with prime order q and generator g. The Diffie-Hellman relation is described as $R^{\text{dh}}_{\text{PP}} = \{(u, s) \in G \times G : s = u^{\alpha}\}$.

A chameleon ABO-EHP system. The public parameter PP is (g, g^{α}) for $g \xleftarrow{\$} G$ and $\alpha \xleftarrow{\$} \mathbb{Z}_q$. The tag space is $\mathcal{T} = \mathbb{Z}_q \times \mathbb{Z}_q$ and the sampling algorithm is $\mathrm{SampR}(r) := (g^r, g^{\alpha r})$, where $r \in \mathbb{Z}_q$. We define $H_{\text{PK}}(\text{TAG}, u) = (g^{\alpha a} \cdot X_1^b \cdot X_2)^r$, where $\text{TAG} = (a, b) \in \mathbb{Z}_q \times \mathbb{Z}_q$ and $\text{PK} = (X_1, X_2) \in G \times G$.

- (Public evaluation/extraction)

- $\mathrm{SetupExt}_{\text{ch}}(\text{PP})$: Pick $\beta_1, \beta_2 \xleftarrow{\$} \mathbb{Z}_q$, then set $\text{PK} = (g^{\beta_1}, g^{\beta_2})$ and $\text{SK} = (\beta_1, \beta_2)$.

- $\mathrm{Pub}_{\text{ch}}(\text{PK}, \text{TAG}, r) = (g^{\alpha a} \cdot X_1^b \cdot X_2)^r$.

- $\mathrm{Ext}_{\text{ch}}(\text{SK}, \text{TAG}, u, \tau) = (\tau \cdot u^{-b\beta_1 - \beta_2})^{a^{-1}}$.

- (Chameleon all-but-one mode)

- $\mathrm{SetupABO}_{\text{ch}}(\text{PP})$: Pick $\beta_1^*, \beta_2^*, x_a, x_b \xleftarrow{\$} \mathbb{Z}_q$ and then set

$$\begin{cases} \text{PK} = (g^{\beta_1^*}(g^{\alpha})^{x_a}, g^{\beta_2^*}(g^{\alpha})^{x_b}), \\ \text{SK}^* = (\beta_1^*, \beta_2^*, x_a, x_b), \\ \mathcal{S} = \{(a, b) \in \mathcal{T} : a + bx_a + x_b = 0 \bmod q\}. \end{cases}$$

- $\mathrm{Priv}_{\text{ch}}(\text{SK}^*, \text{TAG}^*, u) = u^{b\beta_1^* + \beta_2^*}$, where $\text{TAG}^* = (a, b) \in \mathcal{S}$.

- $\mathrm{Ext}^*_{\text{ch}}(\text{SK}^*, \text{TAG}, u, \tau) = \left(\frac{\tau}{u^{b\beta_1^* + \beta_2^*}}\right)^{\frac{1}{a + bx_a + x_b}}$, where $\text{TAG} = (a, b) \in \mathcal{T} \setminus \mathcal{S}$.

- $\mathrm{CompKT}_{\text{ch}}(\text{SK}^*, a) = (-a - x_b) \cdot x_a^{-1} \bmod q$.

Theorem 2. The above construction is a chameleon ABO-EHP system for the DH relation.

The proof of Theorem 2 is given in Appendix B.

Applying the above chameleon ABO-EHP system with pseudorandom generators G_{PP} for DH relation from [1], we may obtain CCA-secure PKE schemes as in [5] under DBDH assumption (see Figure B1 in Appendix B), which is competitive with the hybrid CCA-secure PKE scheme [6].

Extension to the twin DH relation. The twin DH relation with $\text{PP} = (g, g^{\alpha}, g^{\beta})$ is given by

$$R^{\text{2dh}}_{\text{PP}} = \{(u, (s_0, s_1)) \in G \times G^2 : (s_0, s_1) = (u^{\alpha}, u^{\beta})\}.$$

Given $\text{TAG} = (a, b) \in \mathbb{Z}_q \times \mathbb{Z}_q$, $u = g^r \in G$, $\text{PK}=(X_1, X_2, X_3, X_4) \in G^4$ and

$$H_{\text{PK}}(\text{TAG}, u) = \left((g^{\alpha_1 a} \cdot X_1^b \cdot X_2)^r, (g^{\alpha_2 a} \cdot X_3^b \cdot X_4)^r\right),$$

we can similarly construct a chameleon ABO-EHP system for the twin DH relation. If we use the generator $G^{\text{2dh}}_{\text{PP}}(s_0) := \mathrm{GL}(s_0)$ for the twin DH relation, we can obtain a new CCA-secure PKE scheme under the CDH assumption (see Figure B2 in Appendix B). By implementing the trade-off method of [7], we can further obtain a more practical CDH-based PKE scheme with constant ciphertext size (see Figure B3 in Appendix B).

Efficiency comparison of the above schemes is given in Appendix C.

Conclusion. We proposed the notion of chameleon ABO-EHP system, and applied it to construct CCA-secure PKE schemes directly. It also instantiated chameleon ABO-EHP systems for the DH relation and the twin DH relation, which can be used to construct CCA-secure PKE schemes under DBDH assumption and CDH assumption respectively.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61502400, 61571364), Natural Science Foundation of Shaanxi Province (Grant No. 2017JM6037), Seed Foundation of Innovation and Creation for Graduate Students in Northwestern Polytechnical University (Grant No. Z2017022), and National Key R&D Program of China (Grant No. SQ2017YFSF060097).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

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

2 Cash D, Kiltz E, Shoup V. The twin Diffie-Hellman problem and applications. J Cryptol, 2009, 22: 470–504

3 Haralambiev K, Jager T, Kiltz E, et al. 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, Paris, 2010. 1–18

4 Goldreich O, Levin L A. A hard-core predicate for all one-way functions. In: Proceedings of the 21st Annual ACM Symposium on Theory of Computing, Seattle, 1989. 25–32

5 Lai J Z, Deng R H, Liu S L, et al. Efficient CCA-secure PKE from identity-based techniques. In: Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, 2010. 132–147

6 Kang L, Tang X H, Liu J F. Tight chosen ciphertext attack (CCA)-secure hybrid encryption scheme with full public verifiability. Sci China Inf Sci, 2014, 57: 112112

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