SCIENCE CHINA
Information Sciences

• **Supplementary File** •

An efficient $i\mathcal{O}$-based data integrity verification scheme for cloud storage

Lixue SUN[1*], Chunxiang XU[1*], Yuan ZHANG[1,2] & Kefei CHEN[3]

[1] *Center for Cyber Security, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu* 611731*, China;*
[2] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada;*
[3] *School of Science, Hangzhou Normal University, Hangzhou* 310036*, China*

Appendix A Indistinguishability obfuscation

Definition 1 (Indistinguishability Obfuscation). Given a family of polynomial-size circuits $\mathcal{C} = \{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$, an indistinguishability obfuscator for the circuit class $\{\mathcal{C}_\lambda\}$ is defined as a uniform PPT machine $i\mathcal{O}$ that satisfies the following conditions:

- (Preserving Functionality) For all security parameters $\lambda \in \mathbb{N}$, for all $C \in \mathcal{C}_\lambda$, for all inputs x, we have that $\Pr[C'(x) = C(x) : C' \leftarrow i\mathcal{O}(\lambda, C)] = 1$.
- (Indistinguishability of Obfuscation) For any (not necessarily uniform) PPT distinguisher $\mathcal{B} = (Samp, D)$, there exists a negligible function $negl(\cdot)$ such that the following holds: if for all security parameters $\lambda \in \mathbb{N}, \Pr[\forall x, C_0(x) = C_1(x) : (C_0; C_1; \sigma) \leftarrow Samp(1^\lambda)] > 1 - negl(\lambda)$, then we have

$$\begin{aligned}&|\Pr[D(\sigma, i\mathcal{O}(\lambda, C_0)) = 1 : (C_0; C_1; \sigma) \leftarrow Samp(1^\lambda)] - \\ &\Pr[D(\sigma, i\mathcal{O}(\lambda, C_1)) = 1 : (C_0; C_1; \sigma) \leftarrow Samp(1^\lambda)]| \leqslant negl(\lambda).\end{aligned}$$

Appendix B Puncturable pseudorandom functions

A puncturable pseudorandom function (PRF) is evaluated at all bit strings of a certain length. It is defined by two PPT algorithms $(\mathsf{Eval}_F, \mathsf{Puncture}_F)$ that satisfy the following conditions:

- (Functionality preserved under puncturing) For every PPT algorithm $\mathcal{K}$ with input 1^λ outputs a set $S \subseteq \{0,1\}^n$, for all $x \in \{0,1\}^n \backslash S$, we have $\Pr[\mathsf{Eval}_F(K\{S\}, x) = F(K, x) : K \xleftarrow{\$} \mathcal{K}, K\{S\} \leftarrow \mathsf{Puncture}_F(K, S)] = 1$.
- (Pseudorandom at punctured points) For every pair of PPT algorithms $(\mathcal{A}_1, \mathcal{A}_2)$ such that $\mathcal{A}_1(1^\lambda)$ outputs a set $S \subseteq \{0,1\}^n$ and a state σ, consider an experiment where $K \xleftarrow{\$} \mathcal{K}, K\{S\} \leftarrow \mathsf{Puncture}_F(K, S)$. Let U_l denotes the uniform distribution over l bits. Then we have

$$\begin{aligned}&|\Pr[\mathcal{A}_2(\sigma, K\{S\}, S, \mathsf{Eval}_F(K, S)) = 1] - \\ &\Pr[\mathcal{A}_2(\sigma, K\{S\}, S, U_{m(\lambda)\cdot|S|} = 1]| \leqslant negl(\lambda).\end{aligned}$$

* Corresponding author (email: sunlixue2007@sina.com (Lixue SUN), chxxu@uestc.edu.cn (Chunxiang XU))