Derler, David; Slamanig, Daniel

Practical witness encryption for algebraic languages or how to encrypt under Groth-Sahai proofs. (English) Zbl 1408.68057

A language $L \subseteq (0 + 1)^*$ in NP has a witnessing relation $R \subseteq [(0 + 1)^*]^2$ associated such that

$$\forall x \in (0 + 1)^* \ [x \in L \iff \exists w \in (0 + 1)^* : (x, w) \in R].$$

For any word $x \in L$, the corresponding witness $w$ is hard to be found in terms of $x$ itself. A witness encryption (WE) scheme, in rather general terms, consists of two probabilistic polynomial-time maps: an encryption map $Enc : (\text{par}, x, \mu) \mapsto c$, here $\mu$ is a plain text, $c$ is the cipher text and par is a list of parameters, and a decryption map $Dec : (w, c) \mapsto \mu$ such that $((x, w) \in R \implies \Pr[Dec(w, Enc(\text{par}, x, \mu) = \mu)] = 1)$. The words in the language $L$ act as a kind of public keys, while the corresponding witnesses are the private keys.

On the other hand, suppose that for a keyed hash function $h : (k, x) \mapsto v$, where $k$ is a key, $x$ is a plain text and $v$ is the produced hash value, there is constructed, for a language $L$, a corresponding keyed projective hashing map $h_L : (k_L, x, w) \mapsto v$, where $k_L$ is a secondary key depending on the key $k$, such that $((x, w) \in R \implies h_L(k_L, x, w) = h(k, x))$. The hash map is smooth if it is statistically indistinguishable from a uniformly distributed random variable.

In this paper a WE scheme is proposed based the above smooth projective hash functions. Bob (the sender) is ciphering his messages to Alice (the receiver), who should be the unique person able to decipher the received messages. They fix a language $L$. Alice publishes a set $A \subseteq L$ such that for any $x \in A$ Alice is able to find a corresponding witness $w$.

Initially a procedure is given to cipher just a bit $b \in \{0, 1\}$.

Encryption. If $b = 0$, then the cipher text is chosen randomly, else Bob selects a word $x \in A$, generates keys $k$, $k_L$ and the cipher text codifies the tuple consisting of $k_L, x$ and the hashing value $v = h(k, x)$.

Decryption. Alice receives the cipher text and decodifies it in order to extract the hypothetical parts $k_L$, $x$ and the hashing value $v$. Alice finds a corresponding witness $w$ and calculates $v' = h_L(k_L, x, w)$. If $v' = v$ Alice recovers the plain text $b = 1$, otherwise $b = 0$.

Several other parameters may be involved and codified along the protocol.

In order to encrypt messages $\mu$ of arbitrary length, there are also agreed by Alice and Bob a symmetric encryption scheme $\Sigma$, with its own encryption and decryption maps, and a family $\mathcal{H}$ of universal hash functions $H : v \mapsto k \in (0 + 1)^\ell$ where $\ell$ is the length of keys for $\Sigma$.

Encryption. Bob selects a word $x \in A$, generates keys $k$, $k_L$, chooses $H \in \mathcal{H}$ and calculates $v = h(k, x)$, $k = H(v)$ and $\gamma = \Sigma.\text{Enc}(k, \mu)$. The cipher text $C$ codifies the tuple consisting of $\gamma$, $k_L$, $x$ and $H$.

Decryption. Alice receives the cipher text and decodifies it in order to extract the hypothetical parts $\gamma$, $k_L$, $x$ and $H$. She calculates $v' = h_L(k_L, x, w)$ and $k = H(v')$. Then Alice recovers the plain text $\mu = \Sigma.\text{Dec}(\gamma, \gamma)$.

Also several other parameters may be involved and codified along the protocol.

The authors analyze the correctness and robustness of the proposed methods and they consider some particular examples of smooth projective hash functions, families of universal hash functions and special algebraic languages, especially those appearing in the Groth-Sahai non-interactive witness-indistinguishable/zero-knowledge proof framework. The authors emphasize that their methods are practical and robust and the given proofs are sufficient to sustain their claim.

The paper is hard to read due to an abuse of acronyms.

Reviewer: Guillermo Morales Luna (México D. F.)
References:


[37] Kiltz, Eike; Pietrzak, Krzysztof; Stam, Martijn; Yung, Moti, A New Randomness Extraction Paradigm for Hybrid Encryption, 590-609, (2009), Berlin, Heidelberg · Zbl 1239.94065 · doi:10.1007/978-3-642-01001-9_4


[41] Sahai, Amit; Waters, Brent, Fuzzy Identity-Based Encryption, 457-473, (2005), Berlin, Heidelberg · Zbl 1137.94355


[43] Zhandry, Mark, How to Avoid Obfuscation Using Witness PRFs, 421-448, (2015), Berlin, Heidelberg · Zbl 1382.94170