Cryptology ePrint Archive: Report 2011/546

Hidden Vector Encryption Fully Secure Against Unrestricted Queries

Angelo De Caro and Vincenzo Iovino and Giuseppe Persiano

Abstract: Predicate encryption is an important cryptographic primitive (see \cite{BDOP04,BoWa07,Goyal06,KaSaWa08}) that enables fine-grained control on the decryption keys. Roughly speaking, in a predicate encryption scheme the owner of the master secret key $\MSK$ can derive secret key $\SK_P$, for any predicate P from a specified class of predicates $\mathbb{P}$. In encrypting a message M, the sender can specify an {\em attribute} vector $\x$ and the resulting ciphertext $\tilde X$ can be decrypted only by using keys $\SK_P$ such that $P(\x)=1$.

Our main contribution is the {\em first} construction of a predicate encryption scheme that can be proved {\em fully} secure against {\em unrestricted} queries by probabilistic polynomial-time adversaries under non-interactive constant sized (that is, independent of the length ℓ of the attribute vectors) hardness assumptions on bilinear groups of composite order.

Specifically, we consider {\em hidden vector encryption} (HVE in short), a notable case of predicate encryption introduced by Boneh and Waters \cite{BoWa07} and further developed in \cite{ShWa08, IoPe08, SLNHJ10}. In a HVE scheme, the ciphertext attributes are vectors $\x=\langle x_1,\ldots,x_\ell\rangle$ of length ℓ over alphabet Σ, keys are associated with vectors $\y=\langle y_1,\ldots,y_\ell\rangle$ of length ℓ over alphabet $\Sigma\cup\{\star\}$ and we consider the $\Match(\x,\y)$ predicate which is true if and only if, for all i, $y_i\ne\star$ implies $x_i=y_i$. Previous constructions restricted the proof of security to adversaries that could ask only {\em non-matching} queries; that is, for challenge attribute vectors $\x_0$ and $\x_1$, the adversary could ask only for keys of vectors $\y$ for which$\Match(\x_0,\y)=\Match(\x_1,\y)=$ false.

Our proof employs the dual system methodology of Waters \cite{Waters09}, that gave one of the first fully secure construction in this area, blended with a careful design of intermediate security games that keep into account the relationship between challenge ciphertexts and key queries.

Category / Keywords: public-key cryptography / predicate encryption, full security, pairing-based cryptography

Date: received 4 Oct 2011

Contact author: decaro at dia unisa it