Cloud Security
Secure Systems Group

Sara Ramezanian Tommi Meskanen Ville Junnila Roope Vehkalahti Valtteri Niemi

Private Membership Test with Homomorphic Encryption

➢ **Introduction:** Private membership test (PMT) protocols enable clients to query for a certain item in server's database without revealing to the server what the item is. Clients are also prevented from learning anything else about the server's database.

➢ **Protocol:** Our protocol is based on a real world scenario. A server possesses 2^{21} (more than two million) malware samples and stores their SHA-1 values in a database.

Server

- Generates a $2^{16} \times 2^{16}$ matrix $\boldsymbol{M}$ based on the first 32 bits of database elements such that, the first 16 bits determine the rows and the rest of the bits determine the columns of $\boldsymbol{M}$.
- Note that $m_{ij} = (e_i)\boldsymbol{M}(e_j)$ where $\boldsymbol{M}$ is the matrix (m_{ij}) and (e_i) and (e_j) are unit vectors.

Client

- Wants to privately search for an item with SHA-1 value of h.
- Generates secret key s_k and public key p_k.
- ***Encrypts*** the first 32 bits of h utilizing ***homomorphic*** encryption as $\{\alpha_0, \alpha_1, ..., \alpha_{31}\}$

$\{\alpha_0, \alpha_1, ..., \alpha_{31}\}$ and p_k ←

- For any row index i of matrix $\boldsymbol{M}$, computes $\gamma_i = \prod_{k=0}^{15}(\alpha_k + (b_k \oplus 1))$ where the binary representation of i is $i = b_{15}b_{14} \dots b_0$
- For any column index j of matrix $\boldsymbol{M}$, computes $\gamma'_j = \prod_{k=0}^{15}(\alpha_{k+16} + (b_k \oplus 1))$ where $j = b_{15}b_{14} \dots b_0$
- Note that (γ_i) is the encryption of the unit vector (e_i) and (γ'_j) is the encryption of the unit vector (e_j).

❖ The false positive rate of the matrix $\boldsymbol{M}$ is:

$$\frac{2^{21}}{2^{32}} = 0.0004$$

❖ The approximate number of multiplications and additions in server part, respectively are $3 * 2^{16}$ and $2^{16} + 2^{21}$

$$E(m_{ij}) = (\gamma_0 \ \gamma_1 \ \gamma_2 \ \cdots \ \gamma_{65535}) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 \\ & & & & \vdots & & & & & & \vdots \\ & & & & \vdots & & & & & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \gamma'_0 \\ \gamma'_1 \\ \gamma'_2 \\ \vdots \\ \vdots \\ \gamma'_{65535} \end{pmatrix}$$

$\boldsymbol{E(m_{ij})}$ →

- ***Decrypt*** $E(m_{ij})$ with the secret key s_k as c.
- $c = \begin{cases} 0 & \rightarrow h \text{ is not in database} \\ 1 & \rightarrow h \text{ is probably in database} \end{cases}$

➢ **Conclusion:** Homomorphic encryption allows server to search in the matrix without knowledge of client's keys.

✓ A construction of homomorphic encryption scheme can be found in: Van Dijk, Gentry, Halevi, Vaikuntanathan. "Fully homomorphic encryption over the integers. "*Advances in cryptology–EUROCRYPT 2010*. Springer Berlin Heidelberg, 2010. 24-43.

✓ In order to reduce the false positive rate to *1 out of 4 million,* client can repeat the protocol for the next 32 bits of h.

✓ If the client reveals the first 11 bits of h to the server, the false positive rate of the matrix is 0.015 and the security parameter used by the client is ≥ 128, using the implementation of single FPGA setting in Roy et al., the estimated time of one query is 30 seconds.

✓ Roy, Järvinen, Vercauteren, Dimitrov, Verbauwhede. "Modular hardware architecture for somewhat homomorphic function evaluation." *Cryptographic Hardware and Embedded Systems--CHES 2015*. Springer Berlin Heidelberg, 2015. 164-184.

Turun yliopisto
University of Turku
CloSe
Aalto University
Academy of Finland
F-Secure
TRUSTONIC