Homomorphic MAC

Li Chen
lichen.xd at gmail.com
Xidian University
May 22, 2014
Outline

1 Communication Model
   1.1 MAC
   1.2 Homomorphic MAC

2 Algorithm Model

3 Homomorphic MAC Scheme I [1]
   3.1 Basic Construction
References

1 Communication Model

1.1 MAC

(Alice want to sent a message $v$ to Bob)

(Bob received a message $v$, and want to know whether it is sent by Alice)

If $tag' = tag$, Bob believe that $v$ is sent by Alice
1.2 Homomorphic MAC

\[ v^* = c_1 v_1 + c_2 v_2 + \ldots + c_s v_s \]
\[ t^* = c_1 t_1 + c_2 t_2 + \ldots + c_s t_s \]
2 Algorithm Model

A homomorphic MAC scheme includes the following PPT algorithm.

- **MAC**: takes as input a secret key $k$ and a message vector $v$, outputs a tag $t$ for $v$.

- **Verify**: takes as input a 3-tuple $(v, k, t)$, where $k$ is the secret key, $v$ is a message vector, and $t$ is the corresponding tag, output 1 or 0 according to the tag is accepted or not.

- **Combine**: takes as input a sequence of 3-tuple $(v^{(1)}, t^{(1)}, c_1), (v^{(2)}, t^{(2)}, c_2), \cdots, (v^{(r)}, t^{(r)}, c_r)$, where $v^{(i)}$ is the message vector, $t^{(i)}$ is the corresponding tag, and $c_i \in \mathbb{F}_q$ is the combination coefficient. Output a tag $t$ for the vector $v = \sum_{i=1}^{r} c_i v^{(i)}$, satisfying

$$
\text{Verify}\left(\sum_{i=1}^{r} c_i v^{(i)}, k, \text{Combine}((v^{(1)}, t^{(1)}, c_1), \cdots, (v^{(r)}, t^{(r)}, c_r))\right) = 1
$$
3 Homomorphic MAC Scheme I [1]

3.1 Basic Construction

- **MAC:** for a $n$ dimension vector $v = (v_1, \cdots, v_n) \in \mathbb{F}_q^n$, and a $n + l$ dimension secret key $k = (k_1, \cdots, k_{n+l}) \in \mathbb{F}_q^{n+l}$, compute

$$t_j = -\left(\sum_{i=1}^{n} v_i k_i \right) / k_{n+j}$$

for $j = 1, \cdots, l$. Output the corresponding tag $t = (t_1, \cdots, t_l) \in \mathbb{F}_q^l$.

- **Verify:** for a input $(v, k, t)$, check whether

$$t_j = -\left(\sum_{i=1}^{n} v_i k_i \right) / k_{n+j}$$

hold for every $j \in [1, l]$. If do, output 1, otherwise output 0.
Homomorphic MAC Scheme I

- Combine: for the input sequence \((v^{(1)}, t^{(1)}, c_1), \ldots, (v^{(r)}, t^{(r)}, c_r)\), output a tag \(t = \sum_{i=1}^{r} c_i t^{(i)}\).

Correctness: Let \(x^{(i)} = (x_1^{(i)}, \ldots, x_n^{(i)})\), \(i = 1, \ldots, m\) are message vectors, \(t^{(i)} = (t_1^{(i)}, \ldots, t_l^{(i)})\) is the tag corresponding to \(x^{(i)}\). By the algorithm MAC, we have

\[
t_j^{(i)} = - \left( \sum_{h=1}^{n} x_h^{(i)} k_i \right) / k_{n+j}
\]

which is equivalent to

\[
\sum_{h=1}^{n} x_h^{(i)} k_i + t_j^{(i)} k_{n+j} = 0
\]

it follows that

\[
\sum_{i=1}^{m} c_i \left( \sum_{h=1}^{n} x_h^{(i)} k_i \right) + \sum_{i=1}^{m} c_i \left( t_j^{(i)} k_{n+j} \right) = 0
\]
Security: Suppose that an adversary can at most enquire $m$ message vectors $y^{(1)}, \ldots, y^{(m)}$, and obtain their tags $t^{(1)}, \ldots, t^{(m)}$, let $y^{(i)} = (y_1^{(i)}, \ldots, y_n^{(i)})$, and $t^{(i)} = (t_1^{(i)}, \ldots, t_l^{(i)})$, and let $y^{(*)}, t^{(*)}$ are successful forged message vector and tags, then we have the following equations:

\[
\begin{pmatrix}
y^{(1)} & t^{(1)} & 0 & \cdots & 0 \\
y^{(2)} & t^{(2)} & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
y^{(m)} & t^{(m)} & 0 & \cdots & 0 \\
\end{pmatrix}
\cdot k = 0
\]

\[
\begin{pmatrix}
y^{(1)} & 0 & t_2^{(1)} & \cdots & 0 \\
y^{(2)} & 0 & t_2^{(2)} & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
y^{(m)} & 0 & t_2^{(m)} & \cdots & 0 \\
\end{pmatrix}
\cdot k = 0
\]

\[
\begin{pmatrix}
y^{(1)} & 0 & \cdots & 0 & t_l^{(1)} \\
y^{(2)} & 0 & \cdots & 0 & t_l^{(2)} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
y^{(m)} & 0 & \cdots & 0 & t_l^{(m)} \\
\end{pmatrix}
\cdot k = 0
\]

\[
\begin{pmatrix}
y^{(*)} & t^{(*)} & 0 & \cdots & 0 \\
y^{(*)} & 0 & t_2^{(*)} & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
y^{(*)} & 0 & \cdots & 0 & t_l^{(*)} \\
\end{pmatrix}
\cdot k = 0
\]

there are $n + l$ variables $k_1, \ldots, k_{N+l}$, let then rank of the system of the pervious $ml$ equations is $R$, then the rank of the system of the total equations is $R + l$. Therefore, the probability of a successful forging is $\frac{1}{q^l}$. 
Thanks! & Questions?