CC5301-1 Introducción a la Criptografía Moderna
Profesor: Alejandro Hevia A.
Auxiliar: Bryan Ortiz
Estudiante: Andrés Calderón Guardia

Tarea 3

Hashing, MACs, Encriptación Autenticada y Diffie-Hellman

P1. Encriptación Autenticada con Datos Asociados

a) Sea $\mathcal{AE} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ el esquema de encriptación autenticada con datos asociados y un adversario A, partiremos definiendo su juego de confidencialidad IND-CPA modificado de la siguiente forma:

Juego $\text{Izq}^{A}_{\mathcal{AE}}$:	Juego $\text{Der}^{A}_{\mathcal{AE}}$:
PROC Inicializar $K \xleftarrow{\$} \mathcal{G}$ PROC $\text{LR}(M_0, M_1, d)$ $C \xleftarrow{\$} \mathcal{E}_K(M_0, d)$ **return** C	PROC Inicializar $K \xleftarrow{\$} \mathcal{G}$ PROC $\text{LR}(M_0, M_1, d)$ $C \xleftarrow{\$} \mathcal{E}_K(M_1, d)$ **return** C

Con esto podemos definir la ventaja de un adversario A en el sentido IND-CPA de la siguiente forma:

$$\text{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = \left| \Pr\left[\text{Izq}^{A}_{\mathcal{AE}} \Rightarrow 1\right] - \Pr\left[\text{Der}^{A}_{\mathcal{AE}} \Rightarrow 1\right] \right|$$

Ahora definiremos su juego de integridad INT-CTXT modificado a continuación:

Juego $\texttt{INTCTXT}^{A}_{\mathcal{AE}}$:

PROC Inicializar $K \xleftarrow{\$} \mathcal{G}$ $S \leftarrow \emptyset$ PROC $\text{Enc}(M, d)$ $C \xleftarrow{\$} \mathcal{E}_K(M, d)$ $S \leftarrow S \cup \{C\}$ **return** C	PROC $\text{Finalizar}(C, d)$ $M \leftarrow \mathcal{D}_K(C, d)$ **if** $(C \notin S \wedge M \neq \perp)$ **then** **return** true **return** false

De este modo es posible definir otra ventaja para el adversario A, en este caso en el sentido INT-CTXT:

$$\text{Adv}^{\text{int-ctxt}}_{\mathcal{AE}}(A) = \left| \Pr\left[\texttt{INTCTXT}^{A}_{\mathcal{AE}} \Rightarrow \text{true}\right] \right|$$

Entonces, la noción de seguridad que posee la encriptación autenticada con datos asociados se define tal que para un adversario arbitrario A estas dos ventajas sean pequeñas.

b) El esquema de encriptación autenticada con datos asociados planteado se construirá en base a un esquema de encriptación $\mathcal{SE} = (\mathcal{K}, \mathcal{E}', \mathcal{D}')$ seguro en el sentido IND-CPA y un MAC $\mathcal{MA} = (\mathcal{K}', \mathcal{T}, \mathcal{V})$ seguro en el sentido SUF-CMA, además que consideraremos que disponemos de un PRF F:

Alg $\mathcal{G}$:	**Alg** $\mathcal{E}_K(M, d)$:	**Alg** $\mathcal{D}_K(C, d)$:
$K_e \xleftarrow{\$} \mathcal{K}$ $K_m \xleftarrow{\$} \mathcal{K}'$ $K \leftarrow (K_e, K_m)$ **return** K	$c \xleftarrow{\$} \mathcal{E}'_{K_e}(M)$ $t \xleftarrow{\$} \mathcal{T}_{K_m}(c \\| d)$ **return** (c, t)	$(c, t) \leftarrow C$ **if** $\mathcal{V}_{K_m}(c \\| d, t)$ **then** **return** $\mathcal{D}'_{K_e}(c)$ **return** $\perp$

Ahora demostraremos que este esquema es seguro bajo las definiciones anteriores, de modo que primero cabe notar que la propiedad IND-CPA del esquema no depende en que $\mathcal{MA}$ sea SUF-CMA, y asimismo también ocurre para la propiedad INT-CTXT respecto a que $\mathcal{SE}$ sea IND-CPA, por lo que para realizar esta demostración solo se necesita demostrar lo siguiente:

1. $\mathcal{SE}$ `IND-CPA` $\Rightarrow$ $\mathcal{AE}$ `IND-CPA`
2. $\mathcal{MA}$ `SUF-CMA` $\Rightarrow$ $\mathcal{AE}$ `INT-CTXT`

Parte 1. Partiremos demostrando la primera proposición resolviéndola por contradicción, teniendo un $\mathcal{SE}$ que cumple con ser IND-CPA y asumiendo que existe un adversario B tal que posee ventaja significativa en el sentido IND-CPA contra $\mathcal{AE}$.

De esta forma, utilizando B construiremos un adversario A contra $\mathcal{SE}$ en el sentido IND-CPA, en particular usaremos la noción IND-CPA-CG al ser equivalente, el cual posee un oráculo $\mathrm{Fn}_{\mathcal{SE}}$ tal que encripta alguno de los mensajes, de forma que debemos simular MAC para realizar un ataque exitoso:

Adversario A:
  $K_m \xleftarrow{\$} \mathcal{K}'$
  Mientras B envíe mensajes (m_0, m_1) con datos asociados d:
    $c \leftarrow \mathrm{Fn}_{\mathcal{SE}}(m_0, m_1)$
    $t \leftarrow \mathcal{T}_{K_m}(c \| d)$
    $(c, t) \rightarrow B$
  $r \leftarrow B$
  return r

Como se puede ver en el algoritmo el adversario A es capaz de simular perfectamente el oráculo $\mathrm{Fn}_{\mathcal{AE}}$ para B, por lo que A gana el juego INC-CPA-CG con la misma probabilidad que B. Por lo tanto, se tiene:

$$\begin{aligned}
\mathrm{Adv}_{\mathcal{SE}}^{\text{ind-cpa-cg}}(A) &= \mid 2 \cdot \Pr\left[\mathrm{Adivinar}_{\mathcal{SE}}^{A} \Rightarrow \text{true}\right] - 1 \mid \\
&= \mid 2 \cdot \Pr\left[\mathrm{Adivinar}_{\mathcal{AE}}^{B} \Rightarrow \text{true}\right] - 1 \mid \\
&= \mathrm{Adv}_{\mathcal{AE}}^{\text{ind-cpa-cg}}(B)
\end{aligned}$$

Dado que consideramos que B posee ventaja significativa y esta es igual a la ventaja de A, llegamos a una contradicción, por lo que se concluye que el esquema cumple con la confidencialidad IND-CPA definida.

Parte 2. Ahora realizaremos la segunda demostración de forma similar, de modo que tenemos $\mathcal{MA}$ seguro en el sentido SUF-CMA y asumiremos que existe un adversario B contra $\mathcal{AE}$ tal que posee ventaja significativa en el sentido INT-CTXT.

Nuevamente construimos un adversario A contra $\mathcal{MA}$ en el sentido SUF-CMA usando B, tal que posee un oráculo $\mathrm{Tag}_{\mathcal{MA}}$ el cual solamente se encarga de devolver el MAC del mensaje recibido, por lo que para ganar el juego hay que simular adecuadamente la encriptación en el juego INT-CTXT:

Adversario A:
  $K_e \xleftarrow{\$} \mathcal{K}; S' \leftarrow \emptyset$
  Mientras B envíe mensajes m con datos asociados d:
    $c \leftarrow \mathcal{E}'_{K_e}(m)$
    $t \leftarrow \mathrm{Tag}_{\mathcal{MA}}(c \| d)$
    $S' \leftarrow S' \cup \{(c, t)\}$
    $(c, t) \rightarrow B$
  $(c', t') \leftarrow B$
  return $\mathcal{V}_{K_m}(c', t')$

Con esto fuimos nuevamente capaces de simular el juego INT-CTXT sin problemas, considerando que B entrega una tupla (c', t') por la cual no haya preguntado anteriormente, es decir, $(c', t') \notin S'$, de esta forma se tiene:

$$\begin{aligned}
\mathrm{Adv}^{\text{suf-cma}}_{\mathcal{MA}}(A) &= \left| \Pr\left[\texttt{SUF-CMA}^{A}_{\mathcal{MA}} \Rightarrow \text{true}\right] \right| \\
&= \left| \Pr\left[\mathcal{V}_{K_m}(c', t') = 1 \wedge (c', t') \notin S'\right] \right| \\
&= \left| \Pr\left[\mathcal{V}_{K_m}(c', t') = 1 \wedge (c', t') \notin S\right] \right| \\
&\geq \left| \Pr\left[\mathcal{D}_{K_e}(c) \neq \perp \wedge (c', t') \notin S\right] \right| \\
&= \mathrm{Adv}^{\text{int-ctxt}}_{\mathcal{AE}}(B)
\end{aligned}$$

Entonces llegamos a que $\mathrm{Adv}^{\text{suf-cma}}_{\mathcal{MA}}(A) \geq \mathrm{Adv}^{\text{int-ctxt}}_{\mathcal{AE}}(B)$, lo cual indica que $\mathcal{MA}$ no es SUF-CMA seguro, llegando así a la contradicción, por lo que se concluye que este esquema también cumple con ser INT-CTXT seguro.

Finalmente, como se demostraron las dos implicancias se tiene que el esquema cumple con la seguridad definida en el punto anterior.

P2. Resistencia a colisiones

a) Para esta pregunta hay que demostrar que para todo adversario eficiente $\mathcal{A}$ que intenta encontrar una colisión para H, existe un adversario eficiente $\mathcal{B}$ que resuelve el problema del logaritmo discreto en $\mathbb{G}$, tal que:

$$\text{Adv}_H^{\text{cr}}(\mathcal{A}) \leq \text{Adv}_{G,g}^{\text{dl}}(\mathcal{B}) + \frac{1}{q}$$

Para demostrarlo nos aprovecharemos del teorema ♣, de modo que generaremos un algoritmo *busca--relaciones* tal que utilice a este adversario eficiente $\mathcal{A}$, para así tener que su ventaja y la del algoritmo sea la misma. Entonces, la entrada de este algoritmo será G' un conjunto de n elementos pertenecientes a $\mathbb{G}^n$ y $\mathcal{A}_{G'}$ el adversario $\mathcal{A}$ tal que realiza el ataque de colisiones en H usando el conjunto G' como bases, se tiene:

Algoritmo $\mathcal{A}'_{\mathcal{rf}}(G')$:
  $(G'_1, G'_2) \leftarrow \mathcal{A}_{G'}$
  $(x_1, x_2, ..., x_n) \leftarrow G'_1$
  $(x'_1, x'_2, ..., x'_n) \leftarrow G'_2$
  return $(x_1 - x'_1, x_2 - x'_2, ..., x_n - x'_n)$

La justificación de que este algoritmo efectivamente cumple con ser uno *busca-relaciones* es la siguiente, considerando $H_{G'}$ como la función de hash tal que usa el conjunto G' como bases:

$$\begin{aligned}
(x_1, x_2, ..., x_n) \neq (x'_1, x'_2, ..., x'_n), \quad H_{G'}(x_1, x_2, ..., x_n) &= H_{G'}(x'_1, x'_2, ..., x'_n) \\
\Rightarrow g_1^{x_1} \cdot g_2^{x_2} \cdot ... \cdot g_n^{x_n} &= g_1^{x'_1} \cdot g_2^{x'_2} \cdot ... \cdot g_n^{x'_n} \\
\Rightarrow g_1^{x_1 - x'_1} \cdot g_2^{x_2 - x'_2} \cdot ... \cdot g_n^{x_n - x'_n} &= 1
\end{aligned}$$

Y además, es posible notar que la condición $\alpha \neq (0, 0, ..., 0)$ se cumple, dado que $(x_1, x_2, ..., x_n) \neq (x'_1, x'_2, ..., x'_n)$ entonces la resta elemento a elemento de estos dos conjuntos debe tener al menos un resultado distinto de 0, sino ambos conjuntos serían iguales.

De esta forma logramos crear un algoritmo *busca-relaciones* mediante el uso del adversario eficiente $\mathcal{A}$, por lo que es posible concluir lo siguiente:

$$\begin{aligned}
\text{Adv}_{G,g}^{\text{rf}}(\mathcal{A}'_{\mathcal{rf}}) &= \Pr[g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot ... \cdot g_n^{\alpha_n} = 1] \\
&= \Pr\left[\mathtt{CR}_H^{\mathcal{A}} \Rightarrow \text{true}\right] \\
&= \text{Adv}_H^{\text{cr}}(\mathcal{A})
\end{aligned}$$

Con esto es posible evidenciar que si disponemos de un adversario eficiente que encuentra colisiones en H, entonces es posible utilizarlo para crear un algoritmo *busca-relaciones*, por lo que ahora podemos utilizar el teorema ♣ para justificar la existencia de un algoritmo eficiente $\mathcal{B}_{\mathcal{d\ell}}$ que resuelve el problema del logaritmo discreto y es tal que cumple:

$$\text{Adv}_H^{\text{cr}}(\mathcal{A}) = \text{Adv}_{G,g}^{\text{rf}}(\mathcal{A}'_{\mathcal{rf}}) \leq \text{Adv}_{G,g}^{\text{dl}}(\mathcal{B}_{\mathcal{d\ell}}) + \frac{1}{q}$$

Por último, dado que existe dicho algoritmo podemos crear un adversario $\mathcal{B}$ tal que simplemente ocupa dicho algoritmo, con lo cual la ventaja de este adversario y este algoritmo sería la misma, finalmente concluyendo lo siguiente:

$$\text{Adv}_H^{\text{cr}}(\mathcal{A}) \leq \text{Adv}_{G,g}^{\text{dl}}(\mathcal{B}) + \frac{1}{q}$$

b) 🆘