VI EDICIÓN DEL PREMIO "TENGO UN PROYECTO" DEL INSTITUTO DE TECNOLOGÍAS FÍSICAS Y DE LA INFORMACIÓN "LEONARDO TORRES QUEVEDO"

VERIFIABLE COMPUTATION ON ENCRYPTED DATA.

PROYECTO DE FIN DE MÁSTER.

Miguel Morona, Dario Fiore*, Ignacio Cascudo*, Daniele Cozzo*, Maria Emilia Alonso+

* Imdea Software Institute
+ Universidad Complutense de Madrid

ÍNDICE

01

INTRODUCCIÓN

Criptografía y seguridad de la información

La criptografía es una técnica para esconder información a través de canales no seguros. La aparición de la informática y el uso masivo de las comunicaciones digitales, han hecho que la criptografía tenga un mayor carácter relacionado con la computación.

01

INTRODUCCIÓN

Criptografía y seguridad de la información

La criptografía es una técnica para esconder información a través de canales no seguros. La aparición de la informática y el uso masivo de las comunicaciones digitales, han hecho que la criptografía tenga un mayor carácter relacionado con la computación.

Los campos de aplicabilidad son amplios:

- Cifrado homomórfico.
- Protocolos de intercambio de claves.
- Autenticación.
- Firma digitales.
- Criptografía basada en identidad (IBE).
- Protocolos Multi-Party Computation (MPC).
- Computación Verificable.

...

01

INTRODUCCIÓN

Criptografía y seguridad de la información

La criptografía es una técnica para esconder información a través de canales no seguros. La aparición de la informática y el uso masivo de las comunicaciones digitales, han hecho que la criptografía tenga un mayor carácter relacionado con la computación.

Los campos de aplicabilidad son amplios:

- **Cifrado homomórfico.**
- Protocolos de intercambio de claves.
- **Autenticación.**
- Firma digitales.
- Criptografía basada en identidad (IBE).
- Protocolos Multi-Party Computation (MPC).
- **Computación Verificable.**

...

01

INTRODUCCIÓN

Computación Verificable

Un esquema de computación verificable [1] es una técnica criptográfica de vanguardia (state of the art) que pretende eliminar los riesgos de la computación remota y garantizar propiedades como la **corrección** o la **privacidad** de los datos.

[1] Gennaro, R., Gentry, C., & Parno, B. (2010). Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In Advances in Cryptology–CRYPTO 2010: 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings 30 (pp. 465-482). Springer Berlin Heidelberg.

EL PROTOCOLO DE CV

Matemáticamente...

La definición formal de un esquema de **Computación Verificable** consiste en una tupla de algoritmos, cuyo funcionamiento se detalla a continuación:

- $\mathsf{KeyGen}(f, 1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$: Based on the security parameter λ, the randomized key generation algorithm generates a public key which is used by the server to compute f. It also computes a matching secret key, kept in private by the client.
- $\mathsf{ProbGen}_{\mathsf{sk}}(x) \to (\sigma_x, \tau_x)$: The problem generation algorithm uses the secret key sk to encode the input x as a public value σ_x that is given to the server to compute with, and a secret value τ_x which is kept private by the client.
- $\mathsf{Compute}_{\mathsf{pk}}(\sigma_x) \to (\sigma_y)$: Using the client's public key and the encoded input, the server computes an encoded version of the function's output $y = f(x)$.
- $\mathsf{Verify}_{\mathsf{sk}}(\tau_x, \sigma_y) \to (acc, y)$: Using the secret key sk and the secret τ_x, the verification algorithm converts the server's output into a bit acc and a string y. If $acc = 1$ we say the client accepts $y = f(x)$, if $acc = 0$ we say the client rejects.

02

EL PROBLEMA

EL PROBLEMA

Posee datos sensibles que no deben/pueden ser compartidos.

EL PROBLEMA

Posee datos sensibles que no deben/pueden ser compartidos.

EL PROBLEMA

Posee datos sensibles que no deben/pueden ser compartidos.

Quiere una computación sobre los datos de otra persona/organización.

EL PROBLEMA

Posee datos sensibles que no deben/pueden ser compartidos.

Quiere una computación sobre los datos de otra persona/organización.

EL PROBLEMA

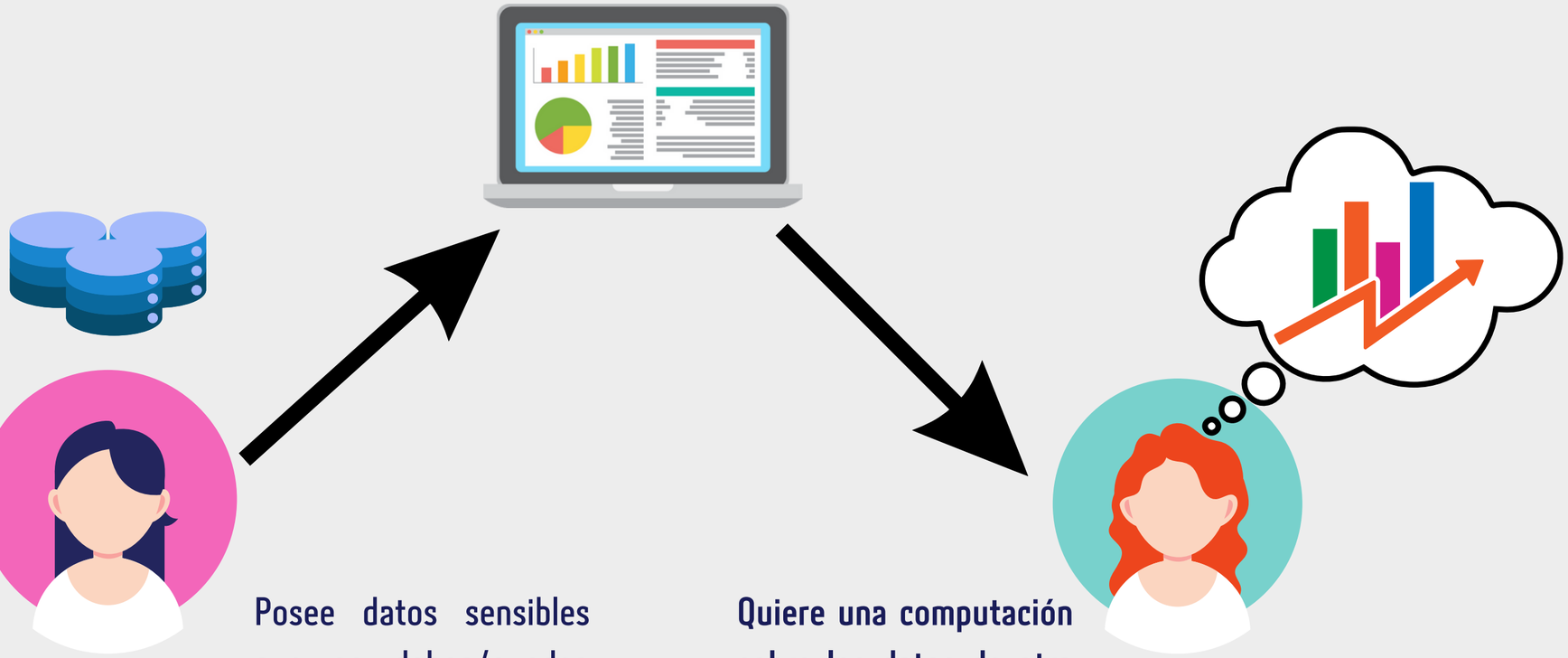
Con poder computacional y conocimiento sobre el procesamiento de los datos.

Posee datos sensibles que no deben/pueden ser compartidos.

Quiere una computación sobre los datos de otra persona/organización.

EL PROBLEMA

Con poder computacional y conocimiento sobre el procesamiento de los datos.



Posee datos sensibles que no deben/pueden ser compartidos.

Quiere una computación sobre los datos de otra persona/organización.

EL PROBLEMA

Con poder computacional y conocimiento sobre el procesamiento de los datos.

Posee datos sensibles que no deben/pueden ser compartidos.

Quiere una computación sobre los datos de otra persona/organización.

EL PROBLEMA

Con poder computacional y conocimiento sobre el procesamiento de los datos.

Posee datos sensibles que no deben/pueden ser compartidos.

Quiere una computación sobre los datos de otra persona/organización.

Varios problemas:

- **PRIVACIDAD:** Damos información sobre nuestros datos privados.

EL PROBLEMA

Con poder computacional y conocimiento sobre el procesamiento de los datos.

Posee datos sensibles que no deben/pueden ser compartidos.

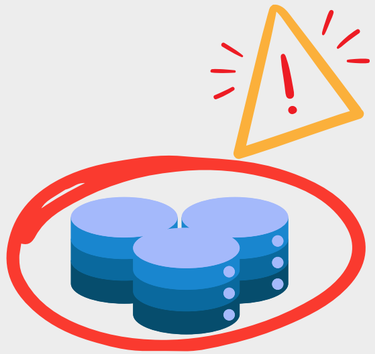
Quiere una computación sobre los datos de otra persona/organización.

Varios problemas:

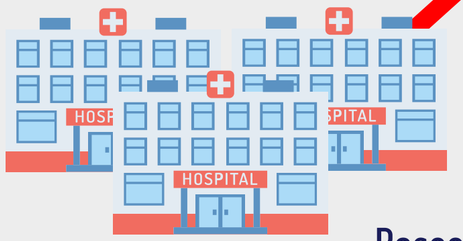
- **PRIVACIDAD:** Damos información sobre nuestros datos privados.

EL PROBLEMA

Con poder computacional y conocimiento sobre el procesamiento de los datos.



CASO REAL



Posee datos sensibles que no deben/pueden ser compartidos.

?

Quiere una computación sobre los datos de otras organizaciones.

Varios problemas:

- **PRIVACIDAD:** Damos información sobre nuestros datos privados.
- **FALSABILIDAD:** No es posible saber si los resultados que (📊) envía son honestamente computados.

SOLUCIÓN PARA LA PRIVACIDAD

03

Encriptación de los datos

SOLUCIÓN PARA LA PRIVACIDAD

03

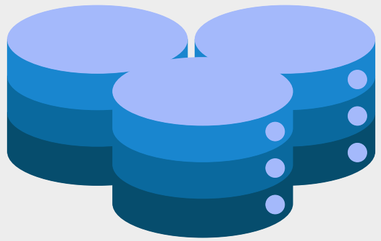
Encriptación de los datos

Para asegurar la privacidad de los datos una de las formas más efectivas y conocidas es hacer uso de un **esquema de encriptación.**

Existen muchos esquemas para encriptar datos, unos más conocidos que otros. En nuestro trabajo nos centraremos en aquellos que tengan una importante propiedad: **Ser Homomórficos**

SOLUCIÓN PARA LA PRIVACIDAD

Esquema de encriptación homomórfica

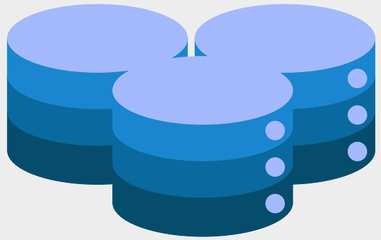


$d_1, \ldots, d_n$

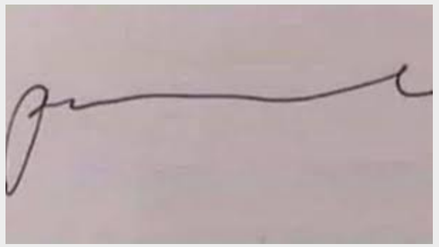
$f(d_1, \ldots, d_n)$

SOLUCIÓN PARA LA PRIVACIDAD

Esquema de encriptación homomórfica



$d_1, \ldots, d_n$



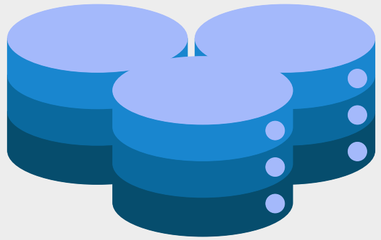
Mundo encriptado

SOLUCIÓN PARA LA PRIVACIDAD

Esquema de encriptación homomórfica

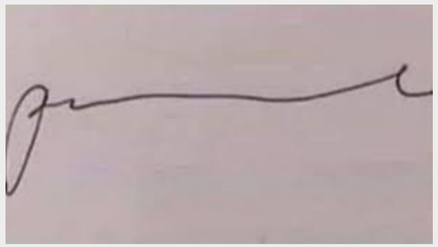
pk

sk

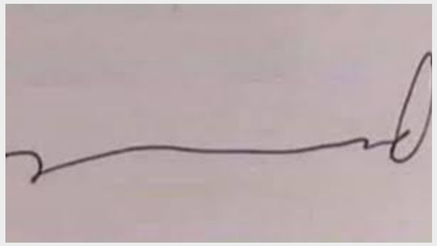


$d_1, \ldots, d_n$

pk



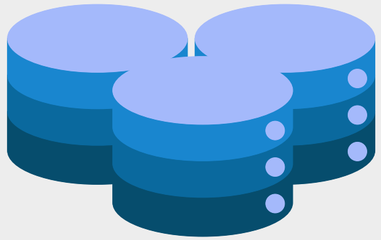
$\dot{f}\left(\dot{d}_1, \ldots, \dot{d}_n\right)$



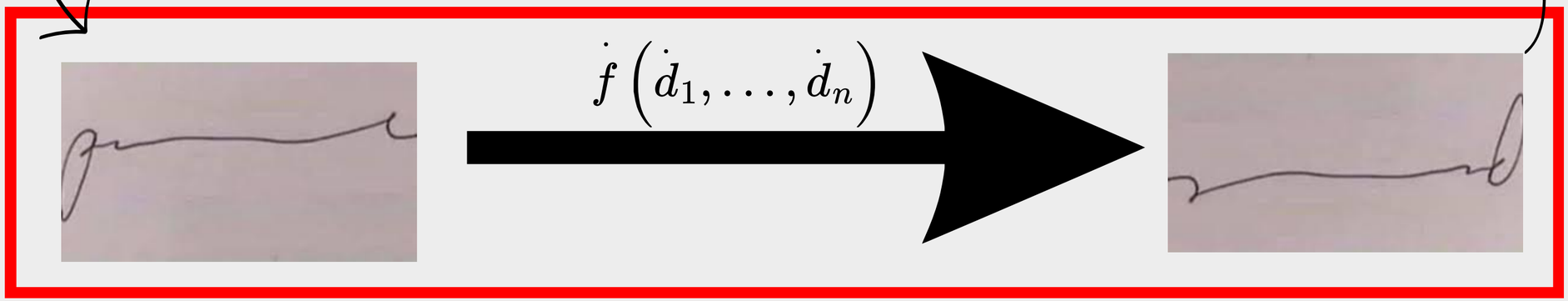
Mundo encriptado

SOLUCIÓN PARA LA PRIVACIDAD

Esquema de encriptación homomórfica



$d_1, \ldots, d_n$



Mundo encriptado

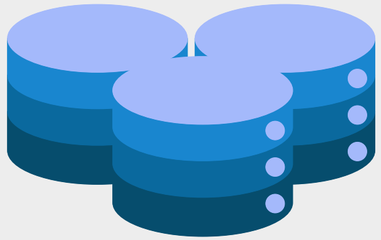
SOLUCIÓN PARA LA PRIVACIDAD

03

Esquema de encriptación homomórfica

pk

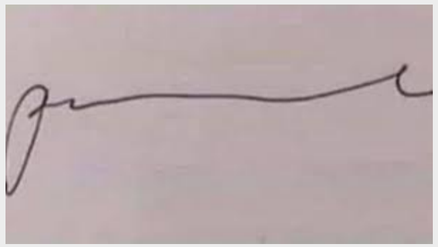
sk



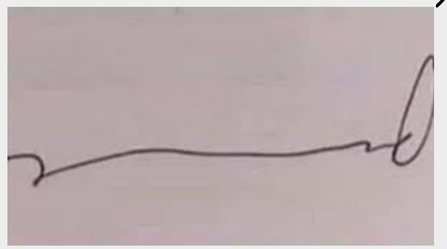
$d_1, \ldots, d_n$

pk

sk



$\dot{f}\left(\dot{d}_1, \ldots, \dot{d}_n\right)$



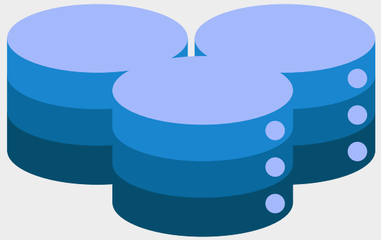
Es seguro ante curiosos...

Mundo encriptado

SOLUCIÓN PARA LA PRIVACIDAD

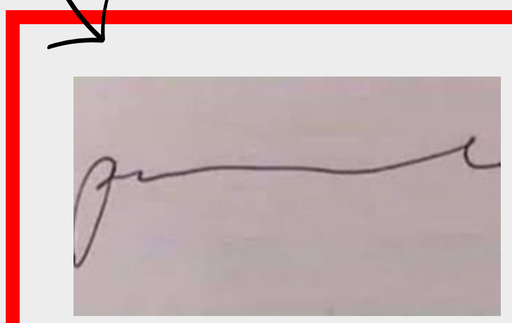
03

Esquema de encriptación homomórfica

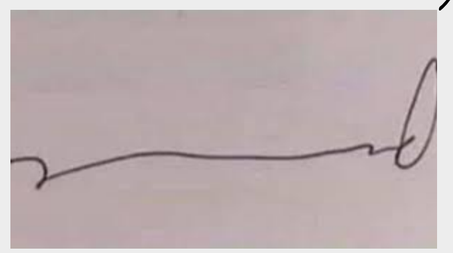


$d_1, \ldots, d_n$

pk



$\dot{f}\left(\dot{d}_1, \ldots, \dot{d}_n\right)$



sk

Mundo encriptado

pk

sk

Se obtienen los mismos resultados

Es seguro ante curiosos...

SOLUCIÓN PARA LA PRIVACIDAD

03

¿Cómo se consigue esto realmente?

SOLUCIÓN PARA LA PRIVACIDAD

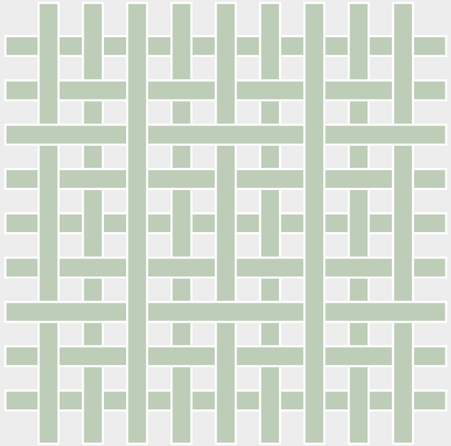
03

¿Cómo se consigue esto realmente?

Para construir un sistema de encriptación que pueda soportar tanto la suma (+) como el producto (*) nos ayudaremos de un problema matemático basado en las celosías.

SOLUCIÓN PARA LA PRIVACIDAD

¿Cómo se consigue esto realmente?



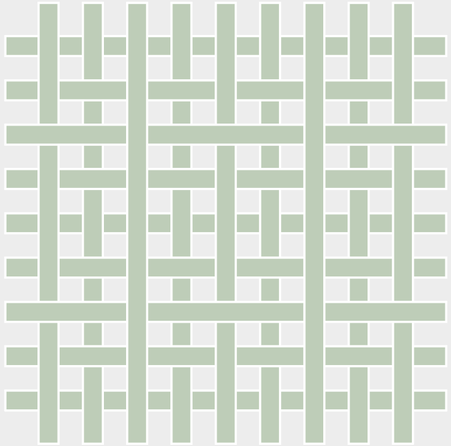
Para construir un sistema de encriptación que pueda soportar tanto la suma (+) como el producto (*) nos ayudaremos de un problema matemático basado en las celosías.

Celosía

SOLUCIÓN PARA LA PRIVACIDAD

03

¿Cómo se consigue esto realmente?



Celosía

Para construir un sistema de encriptación que pueda soportar tanto la suma (+) como el producto (*) nos ayudaremos de un problema matemático basado en las celosías.

Dificultad de resolver un sistema de ecuaciones lineales aproximado

$$
\begin{aligned}
14s_1 + 15s_2 + 5s_3 + 2s_4 &\approx 8 \mod 17\\
13s_1 + 14s_2 + 14s_3 + 6s_4 &\approx 16 \mod 17\\
6s_1 + 10s_2 + 13s_3 + 1s_4 &\approx 3 \mod 17\\
10s_1 + 4s_2 + 12s_3 + 16s_4 &\approx 12 \mod 17\\
9s_1 + 5s_2 + 9s_3 + 6s_4 &\approx 9 \mod 17\\
3s_1 + 6s_2 + 4s_3 + 5s_4 &\approx 16 \mod 17\\
&\vdots\\
6s_1 + 7s_2 + 16s_3 + 2s_4 &\approx 3 \mod 17
\end{aligned}
$$

RLWE

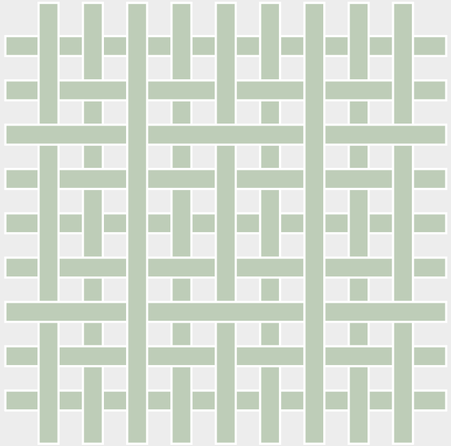
Trabajando en aritmética modular y si *s* es más grande [3] ... Es un poco más complicado.

[3] Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 56(6), 1-40.

SOLUCIÓN PARA LA PRIVACIDAD

03

¿Cómo se consigue esto realmente?



Celosía

Para construir un sistema de encriptación que pueda soportar tanto la suma (+) como el producto (*) nos ayudaremos de un problema matemático basado en las celosías.

Dificultad de resolver un sistema de ecuaciones lineales aproximado

$$
\begin{aligned}
14s_1 + 15s_2 + 5s_3 + 2s_4 &\approx 8 \mod 17\\
13s_1 + 14s_2 + 14s_3 + 6s_4 &\approx 16 \mod 17\\
6s_1 + 10s_2 + 13s_3 + 1s_4 &\approx 3 \mod 17\\
10s_1 + 4s_2 + 12s_3 + 16s_4 &\approx 12 \mod 17\\
9s_1 + 5s_2 + 9s_3 + 6s_4 &\approx 9 \mod 17\\
3s_1 + 6s_2 + 4s_3 + 5s_4 &\approx 16 \mod 17\\
&\vdots\\
6s_1 + 7s_2 + 16s_3 + 2s_4 &\approx 3 \mod 17
\end{aligned}
$$

RLWE

Trabajando en aritmética modular y si *s* es más grande [3] ... Es un poco más complicado.

[3] Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 56(6), 1-40.

$$\boldsymbol{s} = (0, 13, 9, 11).$$

SOLUCIÓN PARA LA PRIVACIDAD

¿Cómo se consigue esto realmente?

Por simplicidad, consideraremos el esquema BV11 [4].

[4] Brakerski, Z., & Vaikuntanathan, V. (2011, August). Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Annual cryptology conference (pp. 505-524). Berlin, Heidelberg: Springer Berlin Heidelberg.

Zvika Brakerski

Vinod Vaikuntanathan

SOLUCIÓN PARA LA PRIVACIDAD

¿Cómo se consigue esto realmente?

Por simplicidad, consideraremos el esquema BV11.

Zvika Brakerski

Vinod Vaikuntanathan

- $\mathsf{BV.KeyGen}(1^\lambda) \rightarrow (\mathsf{pk}, \mathsf{sk})$: sample a secret key $\mathsf{sk} = s \xleftarrow{\$} \chi$ and a public key $\mathsf{pk} = (a_0, b_0 = a_0 s + te_0)$ where $a_0 \xleftarrow{\$} \mathcal{R}_q$ and $e_0 \xleftarrow{\$} \chi$.

- $\mathsf{BV.Enc}(\mathsf{pk}, m) \rightarrow (c)$: sample $v, e' \xleftarrow{\$} \chi$ and $e'' \xleftarrow{\$} \chi'$ where χ' is the same as χ but with standard deviation $\sigma' > 2^{\omega(logN)} \cdot \sigma$. Then compute $(a, b) = (a_0 v + te', b_0 v + te'') \in \mathcal{R}_q^2$. Output $c = (c_0, c_1, 0, \ldots, 0) \in \mathcal{R}_q^D$ where:

$$c_0 = m + b \ , \ \ c_1 = -a$$

- $\mathsf{BV.Dec}(\mathsf{sk}, m) \rightarrow (c)$: Using the secret key $\mathsf{sk} = s$, compute $c(s) = \sum_{i=0}^{D-1} c_i s^i$ and output $m = c(s) \ mod \ t$.

- $\mathsf{BV.Eval}(g, c_1, \ldots, c_r) \rightarrow c_g$: addition and multiplication of two ciphertexts $c = \mathsf{Enc}(m)$, $c' = \mathsf{Enc}(m') \in \mathcal{R}_q^D$ are defined as the usual addition and multiplication in $\mathcal{R}_q[Y]$:

  - $c^{(1)} + c^{(2)} = (c_0^{(1)} + c_0^{(2)}, \ldots, c_{D-1}^{(1)} + c_{D-1}^{(2)})$ encrypts $m + m'$.
  - for the multiplication of two ciphertexts $c^* = c^{(1)} \cdot c^{(2)} = (c_0^*, \ldots, c_{D-1}^*)$ we calculate by the convolution operator: $\forall k = 0, \ldots, D-1$, compute $c_k^* = \sum_{i=0}^{k} c_i^{(1)} \cdot c_{k-i}^{(2)}$

SOLUCIÓN PARA LA FALSABILIDAD

04

Message Authenticator Codes (MAC)

SOLUCIÓN PARA LA FALSABILIDAD

- Message Authenticator Codes (MAC)

SOLUCIÓN PARA LA FALSABILIDAD

04

Message Authenticator Codes (MAC)

Los MACs es una herramienta criptográfica para asegurar la autoría de un mensaje.

SOLUCIÓN PARA LA FALSABILIDAD

04

Message Authenticator Codes (MAC)

Los MACs es una herramienta criptográfica para asegurar la autoría de un mensaje.

SOLUCIÓN PARA LA FALSABILIDAD

04

Message Authenticator Codes (MAC)

Los MACs es una herramienta criptográfica para asegurar la autoría de un mensaje.

Existen diferentes tipos de construcciones para estos elementos. Por conveniencia, necesitaremos aquellos que cumplan la propiedad de **manipulabilidad.**

SOLUCIÓN PARA LA FALSABILIDAD

04

Message Authenticator Codes (MAC)

Los MACs es una herramienta criptográfica para asegurar la autoría de un mensaje.

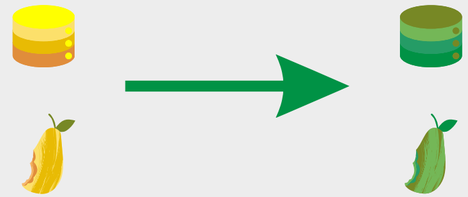
Existen diferentes tipos de construcciones para estos elementos. Por conveniencia, necesitaremos aquellos que cumplan la propiedad de **manipulabilidad.**

SOLUCIÓN PARA LA FALSABILIDAD

Message Authenticator Codes (MAC)

Los MACs es una herramienta criptográfica para asegurar la autoría de un mensaje.

Existen diferentes tipos de construcciones para estos elementos. Por conveniencia, necesitaremos aquellos que cumplan la propiedad de **manipulabilidad.**

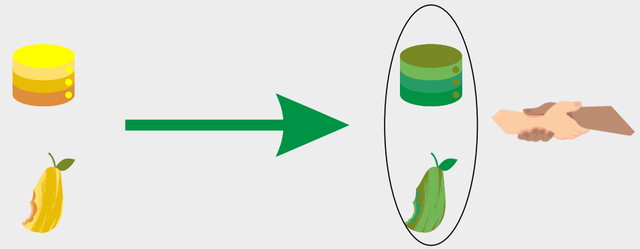


SOLUCIÓN PARA LA FALSABILIDAD

Message Authenticator Codes (MAC)

Los MACs es una herramienta criptográfica para asegurar la autoría de un mensaje.

Existen diferentes tipos de construcciones para estos elementos. Por conveniencia, necesitaremos aquellos que cumplan la propiedad de **manipulabilidad.**



SOLUCIÓN PARA LA FALSABILIDAD

04

Matemáticamente...

SOLUCIÓN PARA LA FALSABILIDAD

04

Matemáticamente...

Para autenticar un mensaje, en la literatura podemos encontrar esta construcción por Catalano y Fiore (CF13) [5].

Dario Catalano

Dario Fiore

[5] Catalano, D., & Fiore, D. (2013, May). Practical homomorphic MACs for arithmetic circuits. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 336-352). Berlin, Heidelberg: Springer Berlin Heidelberg.

SOLUCIÓN PARA LA FALSABILIDAD

Matemáticamente...

Para autenticar un mensaje, en la literatura podemos encontrar esta construcción por Catalano y Fiore (CF13).

Dario Catalano

Dario Fiore

$$CF13: \mathbb{Z}_q \rightarrow \mathbb{Z}_q^2$$

SOLUCIÓN PARA LA FALSABILIDAD

Matemáticamente...

Para autenticar un mensaje, en la literatura podemos encontrar esta construcción por Catalano y Fiore (CF13).

Dario Catalano

Dario Fiore

$$CF13: \mathbb{Z}_q \rightarrow \mathbb{Z}_q^2$$

ek = p

vk = (K, x)

$\tau \leftarrow CRS()$

$r_\tau = F_K(\tau)$

$x \leftarrow Z_p$

$$m \mapsto \left(m, \frac{m - r_\tau}{x}\right)$$

SOLUCIÓN PARA LA FALSABILIDAD

Matemáticamente...

Para autenticar un mensaje, en la literatura podemos encontrar esta construcción por Catalano y Fiore (CF13).

Dario Catalano

Dario Fiore

$$\text{CF13}: \quad \mathbb{Z}_q \rightarrow \mathbb{Z}_q^2$$

ek = p

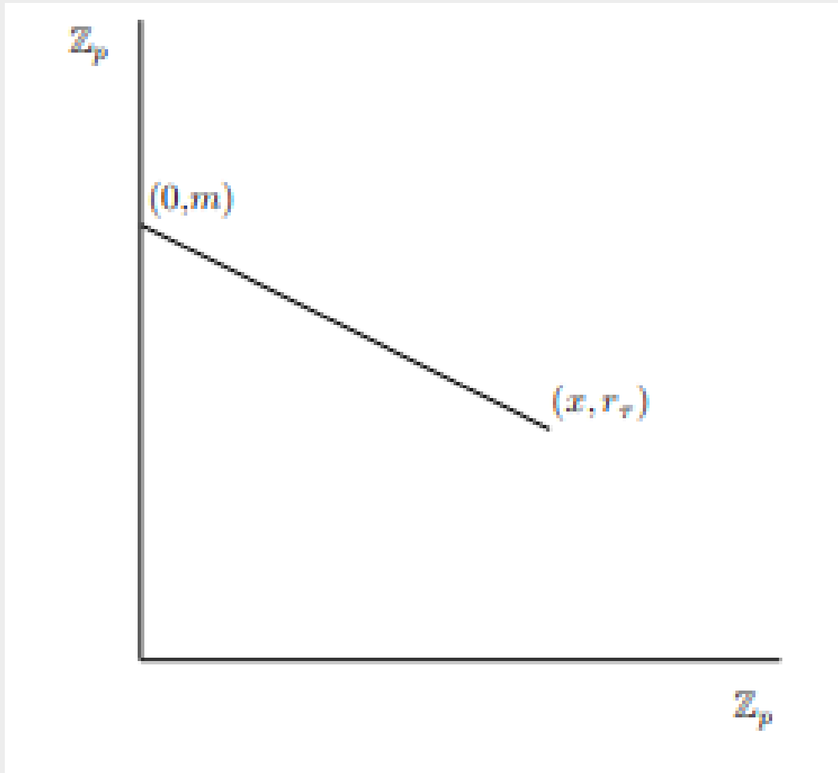
vk = (K, x)

$\tau \leftarrow CRS\,()$

$r_\tau = F_K\,(\tau)$

$x \leftarrow Z_p$

$$m \mapsto \left(m, \frac{m - r_\tau}{x}\right)$$



$$P\,(y) = m + \frac{m - r_\tau}{x} \times y$$

SOLUCIÓN PARA LA FALSABILIDAD

04

Matemáticamente...

Para autenticar un mensaje, en la literatura podemos encontrar esta construcción por Catalano y Fiore (CF13).

Dario Catalano

Dario Fiore

$$CF13: \ \mathbb{Z}_q \rightarrow \mathbb{Z}_q^2$$

ek = p

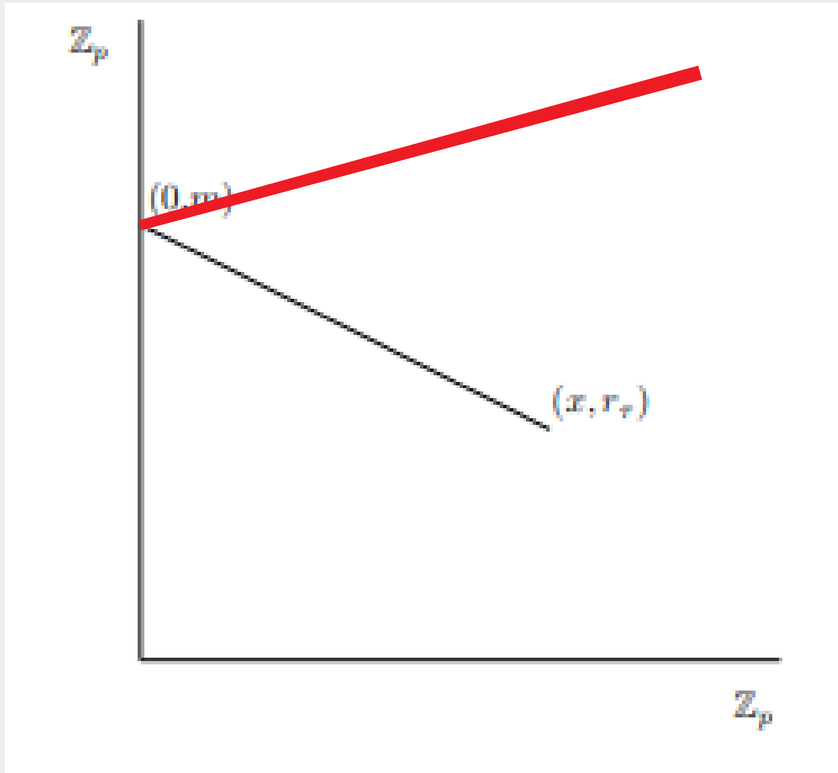
vk = (K, x)

$\tau \leftarrow CRS()$

$r_\tau = F_K(\tau)$

$x \leftarrow Z_p$

$$m \mapsto \left(m, \frac{m - r_\tau}{x}\right)$$



$$P(y) = m + \frac{m - r_\tau}{x} \times y$$

SOLUCIÓN PARA LA FALSABILIDAD

Matemáticamente...

Para autenticar un mensaje, en la literatura podemos encontrar esta construcción por Catalano y Fiore (CF13).

Dario Catalano

Dario Fiore

$$\text{CF13}: \quad \mathbb{Z}_q \rightarrow \mathbb{Z}_q^2$$

ek = p

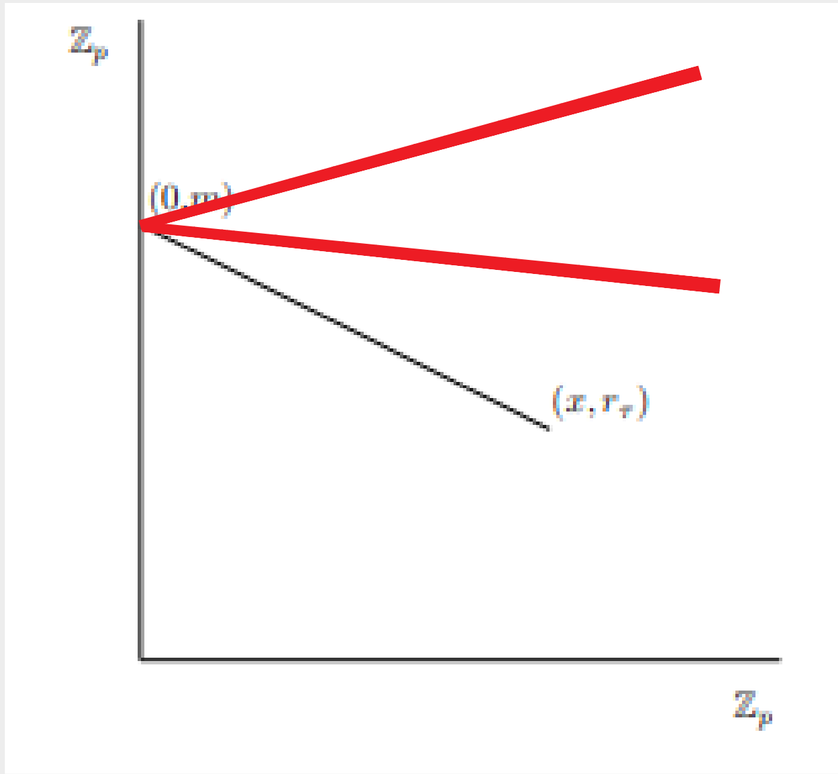
vk = (K, x)

$\tau \leftarrow CRS\,()$

$r_\tau = F_K\,(\tau)$

$x \leftarrow Z_p$

$$m \mapsto \left(m, \frac{m - r_\tau}{x}\right)$$



$$P\,(y) = m + \frac{m - r_\tau}{x} \times y$$

SOLUCIÓN PARA LA FALSABILIDAD

Matemáticamente...

Para autenticar un mensaje, en la literatura podemos encontrar esta construcción por Catalano y Fiore (CF13).

Dario Catalano

Dario Fiore

$$CF13: \quad \mathbb{Z}_q \rightarrow \mathbb{Z}_q^2$$

ek = p

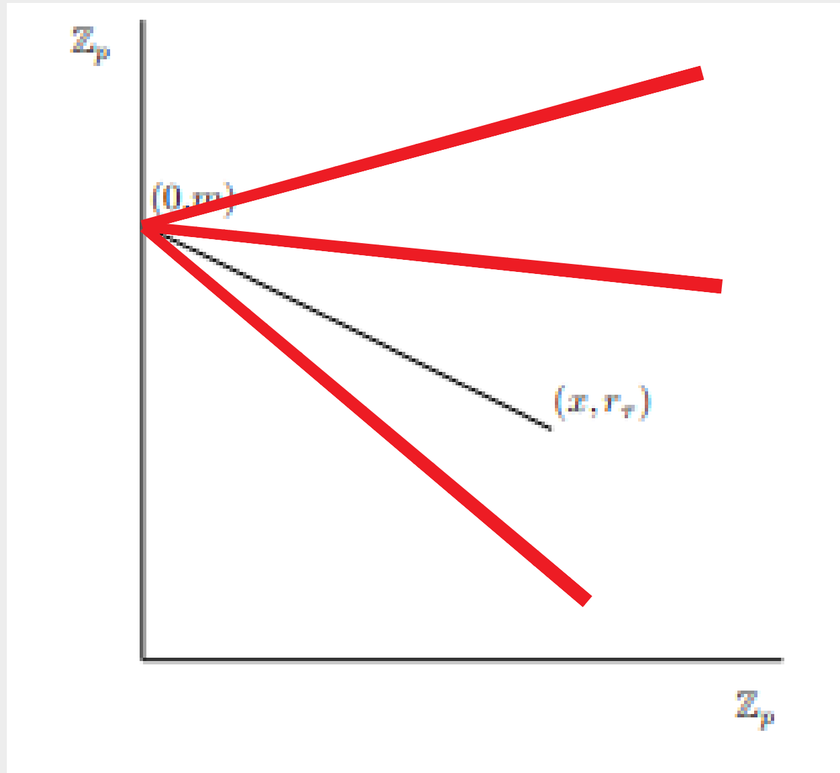
vk = (K, x)

$\tau \leftarrow CRS()$

$r_\tau = F_K(\tau)$

$x \leftarrow Z_p$

$$m \mapsto \left(m, \frac{m - r_\tau}{x}\right)$$



$$P(y) = m + \frac{m - r_\tau}{x} \times y$$

SOLUCIÓN PARA LA FALSABILIDAD

Matemáticamente...

Para autenticar un mensaje, en la literatura podemos encontrar esta construcción por Catalano y Fiore (CF13).

Dario Catalano

Dario Fiore

$$\text{CF13}: \quad \mathbb{Z}_q \rightarrow \mathbb{Z}_q^2$$

ek = p

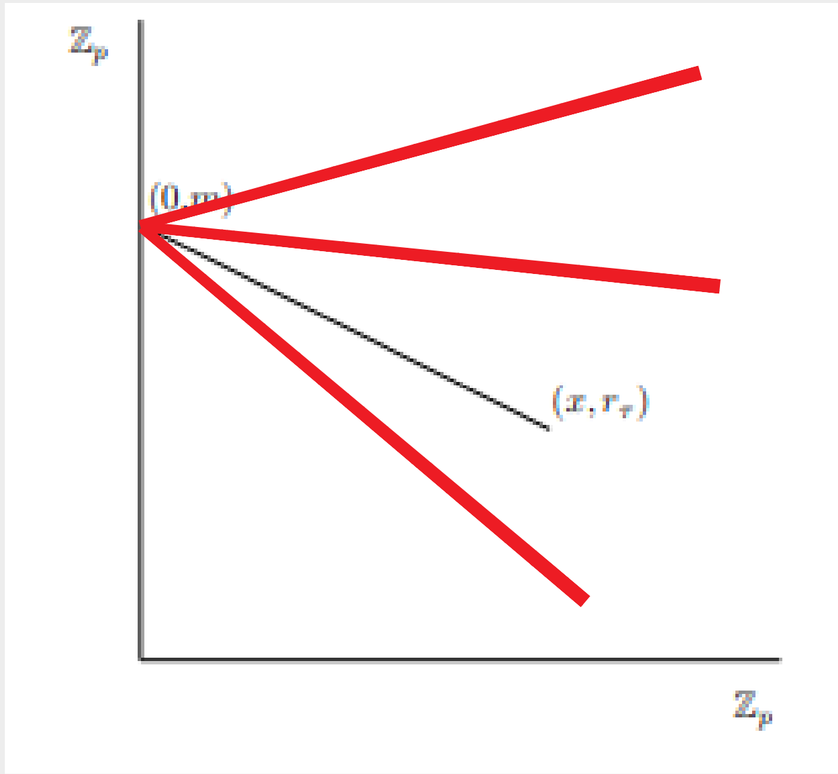
vk = (K, x)

$\tau \leftarrow CRS\,()$

$r_\tau = F_K\,(\tau)$

$x \leftarrow Z_p$

$$m \mapsto \left(m, \frac{m - r_\tau}{x}\right)$$



Sin embargo, para nuestros intereses trataremos de autenticar los “ciphertexts” o textos cifrados ya que CF13 expone el mensaje *m* en una de sus componentes.

$$P\,(y) = m + \frac{m - r_\tau}{x} \times y$$

SOLUCIÓN PARA LA FALSABILIDAD

Matemáticamente...

Para autenticar un mensaje, en la literatura podemos encontrar esta construcción por Catalano y Fiore (CF13).

Dario Catalano

Dario Fiore

$$\text{CF13}: \quad \mathbb{Z}_q \rightarrow \mathbb{Z}_q^2$$

ek = p

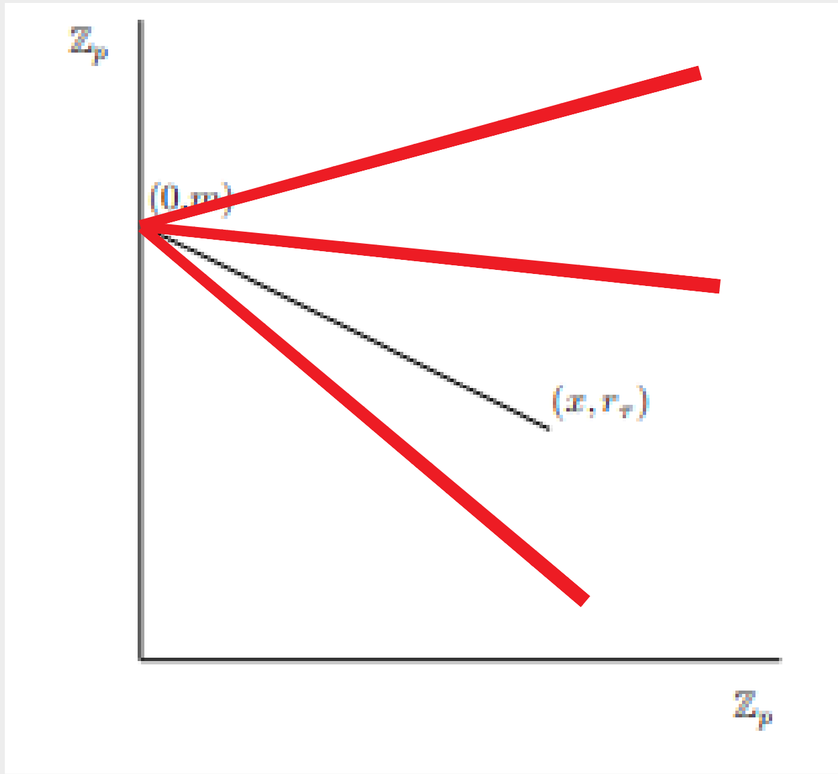
vk = (K, x)

$\tau \leftarrow CRS\,()$

$r_\tau = F_K\,(\tau)$

$x \leftarrow Z_p$

$$c \mapsto \left(c, \frac{c - r_\tau}{x}\right)$$



Sin embargo, para nuestros intereses trataremos de autenticar los “ciphertexts” o textos cifrados ya que CF13 expone el mensaje *m* en una de sus componentes.

$$P\,(y) = m + \frac{m - r_\tau}{x} \times y$$

EL PROTOCOLO DE CV SEGURO

BV11: $R_t \mapsto R_q^2$

CF13: $Z_q \mapsto Z_q^2$

EL PROTOCOLO DE CV SEGURO

BV11: $R_t \mapsto R_q^2$

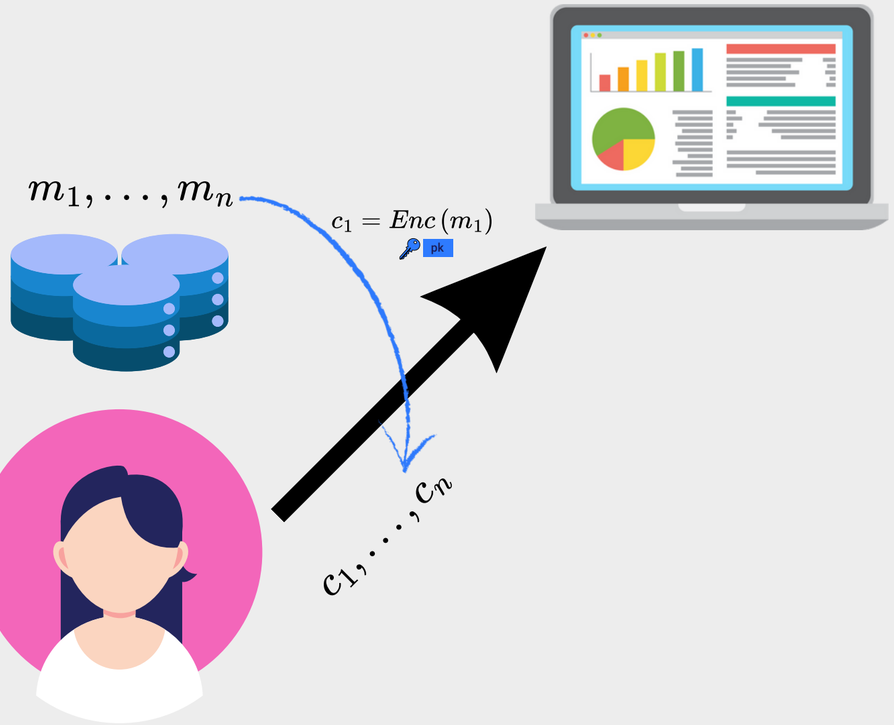
CF13: $Z_q \mapsto Z_q^2$

$m_1, \ldots, m_n$

EL PROTOCOLO DE CV SEGURO

BV11: $R_t \mapsto R_q^2$

CF13: $Z_q \mapsto Z_q^2$



EL PROTOCOLO DE CV SEGURO

05

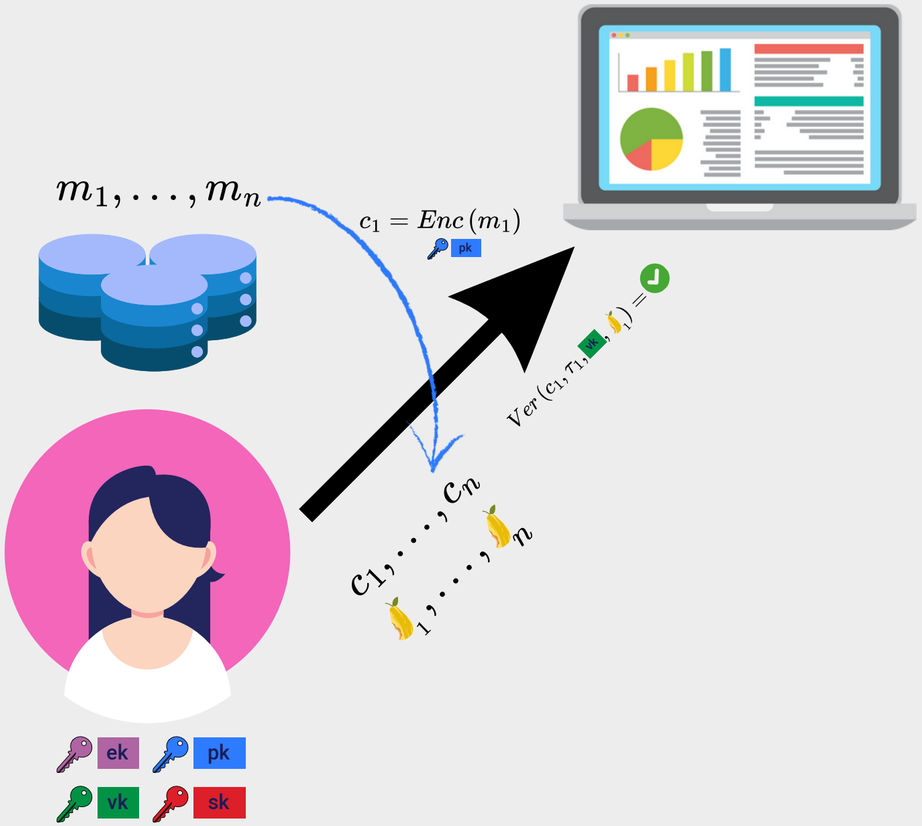
BV11: $R_t \mapsto R_q^2$

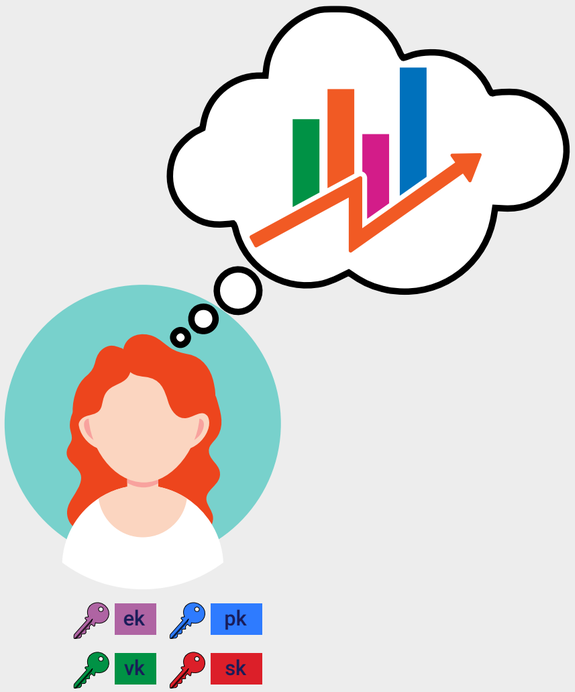
CF13: $Z_q \mapsto Z_q^2$

EL PROTOCOLO DE CV SEGURO

BV11: $R_t \mapsto R_q^2$

CF13: $Z_q \mapsto Z_q^2$





EL PROTOCOLO DE CV SEGURO

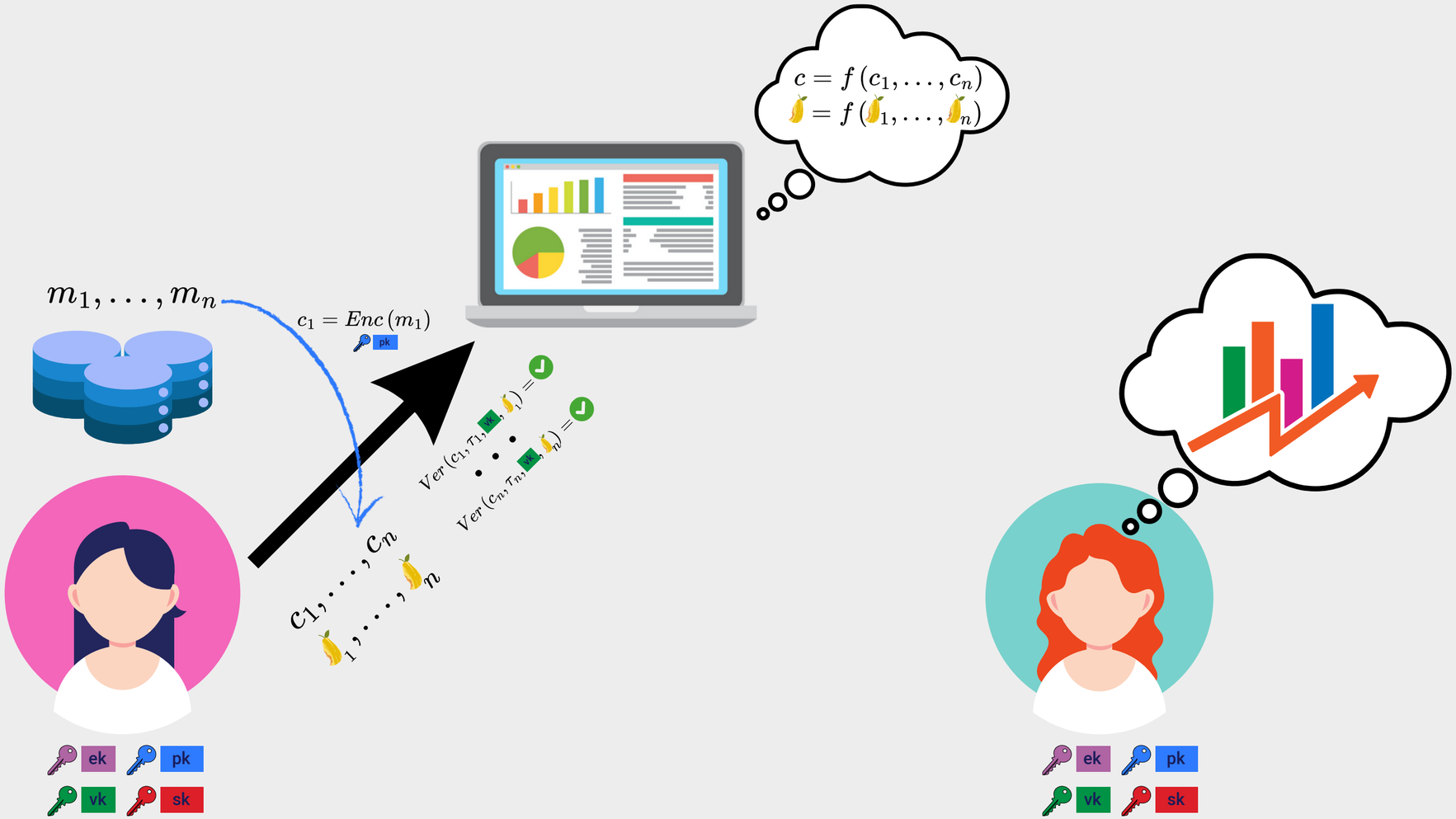
BV11: $R_t \mapsto R_q^2$

CF13: $Z_q \mapsto Z_q^2$

EL PROTOCOLO DE CV SEGURO

BV11: $R_t \mapsto R_q^2$

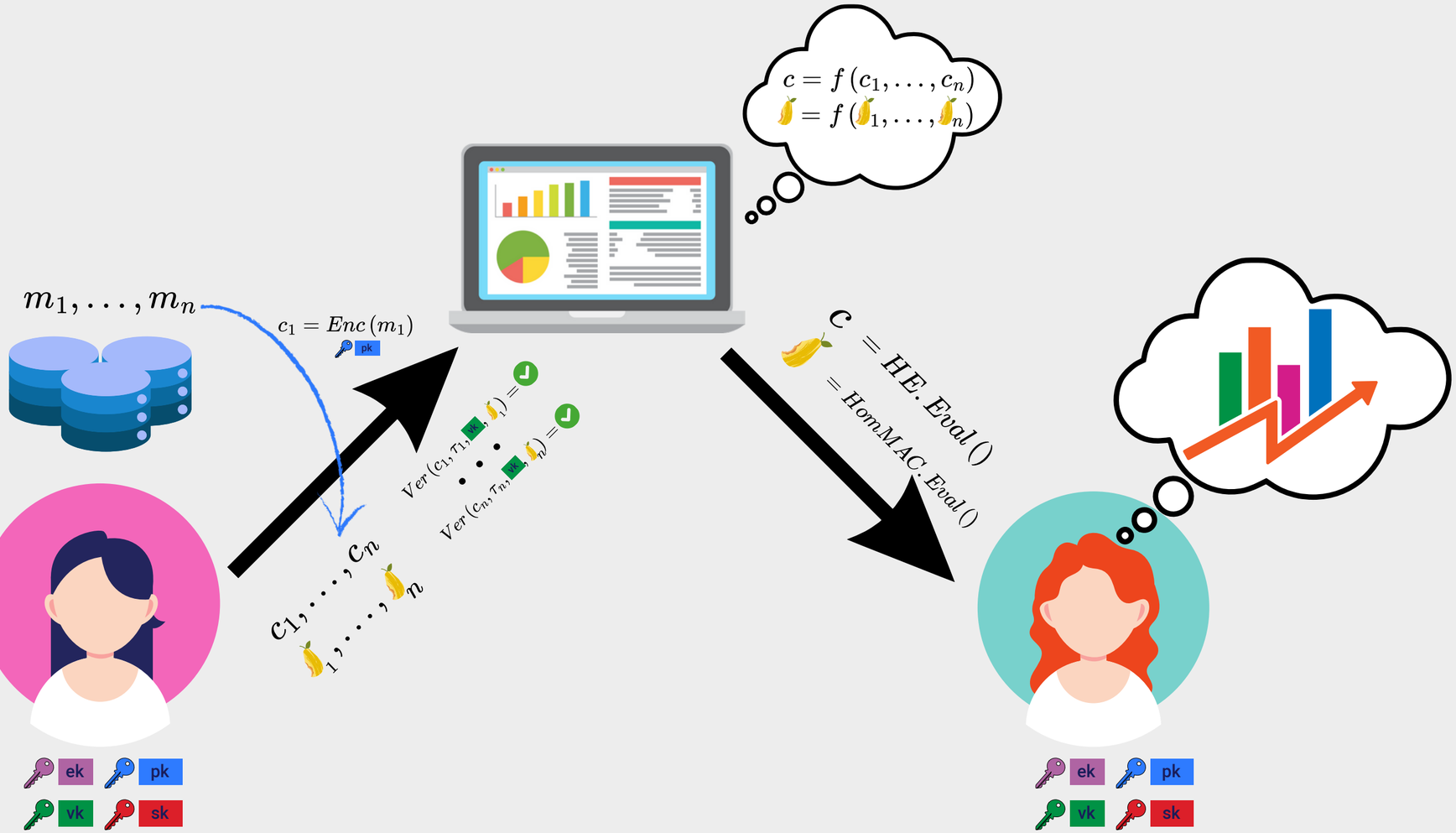
CF13: $Z_q \mapsto Z_q^2$



EL PROTOCOLO DE CV SEGURO

BV11: $R_t \mapsto R_q^2$

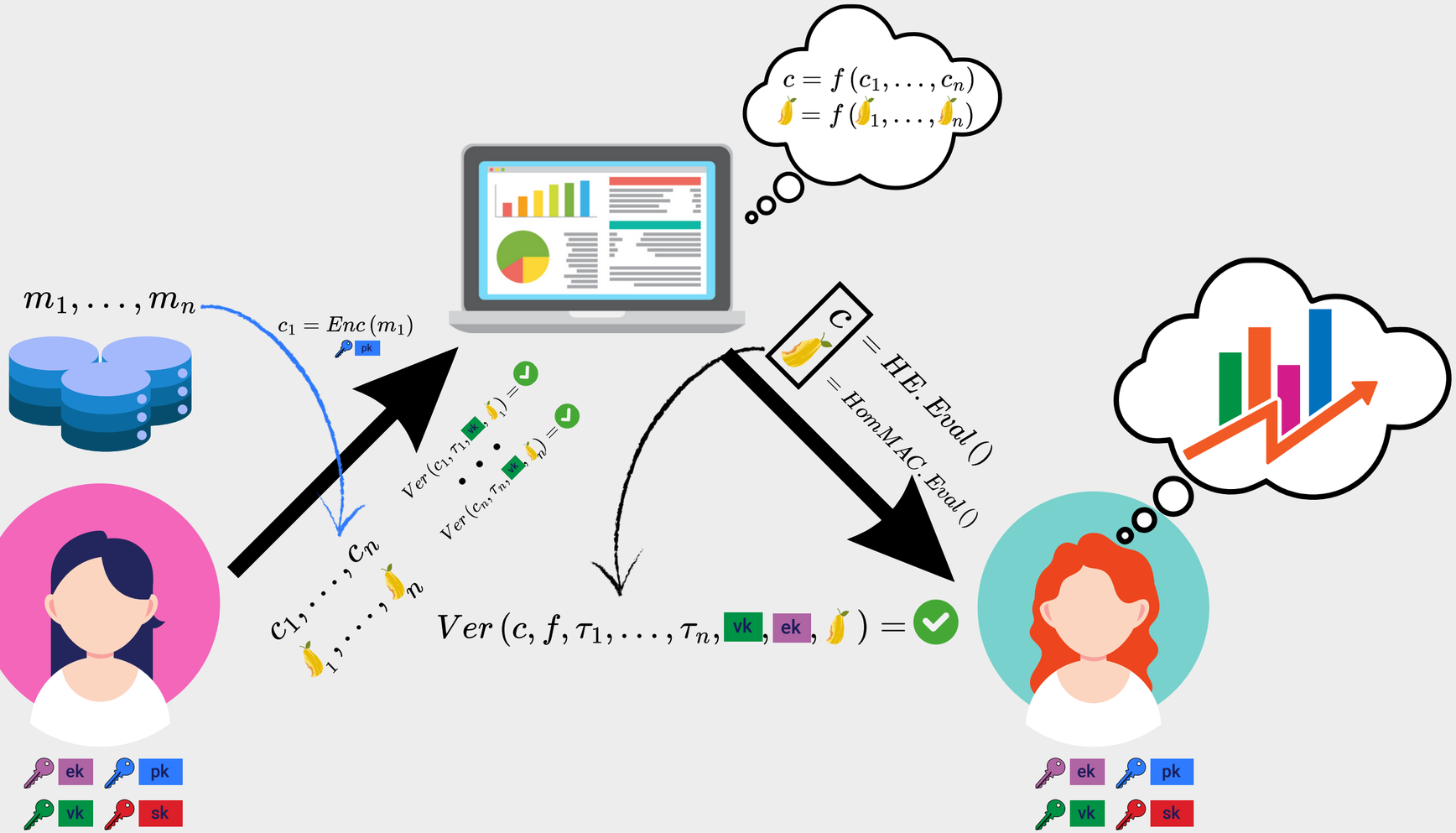
CF13: $Z_q \mapsto Z_q^2$



EL PROTOCOLO DE CV SEGURO

BV11: $R_t \mapsto R_q^2$

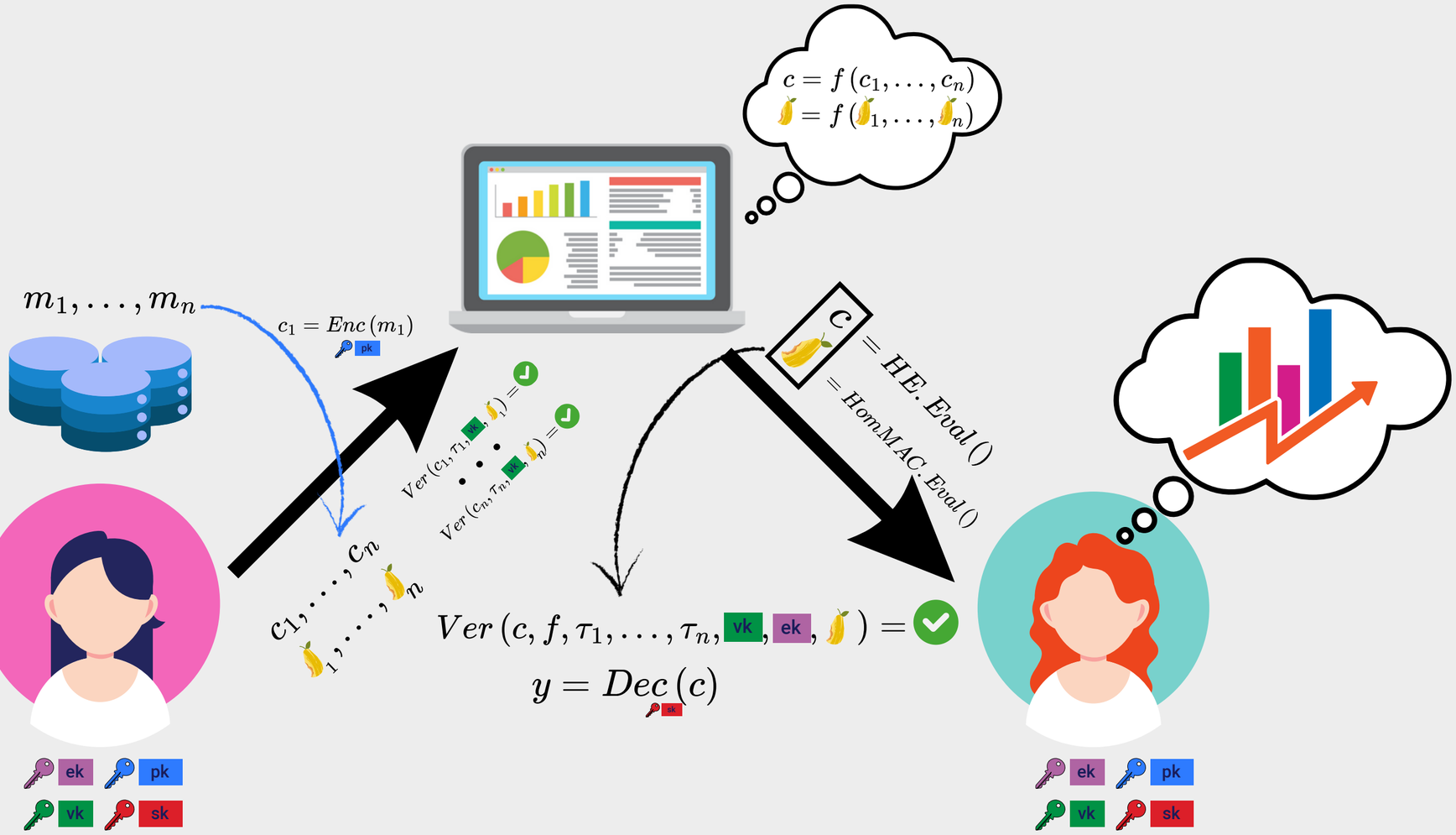
CF13: $Z_q \mapsto Z_q^2$



EL PROTOCOLO DE CV SEGURO

BV11: $R_t \mapsto R_q^2$

CF13: $Z_q \mapsto Z_q^2$



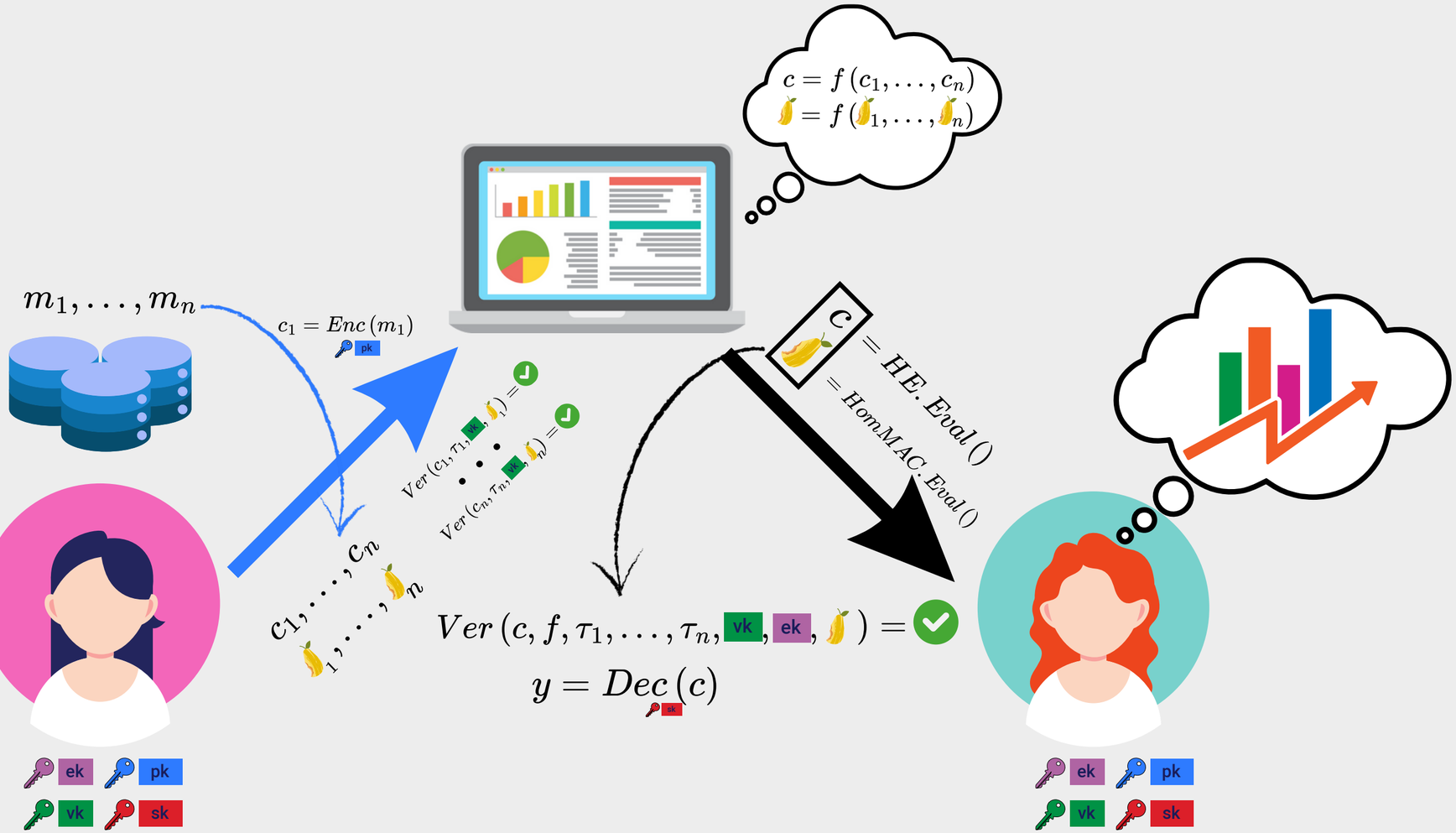
EL PROTOCOLO DE CV SEGURO

BV11: $R_t \mapsto R_q^2$

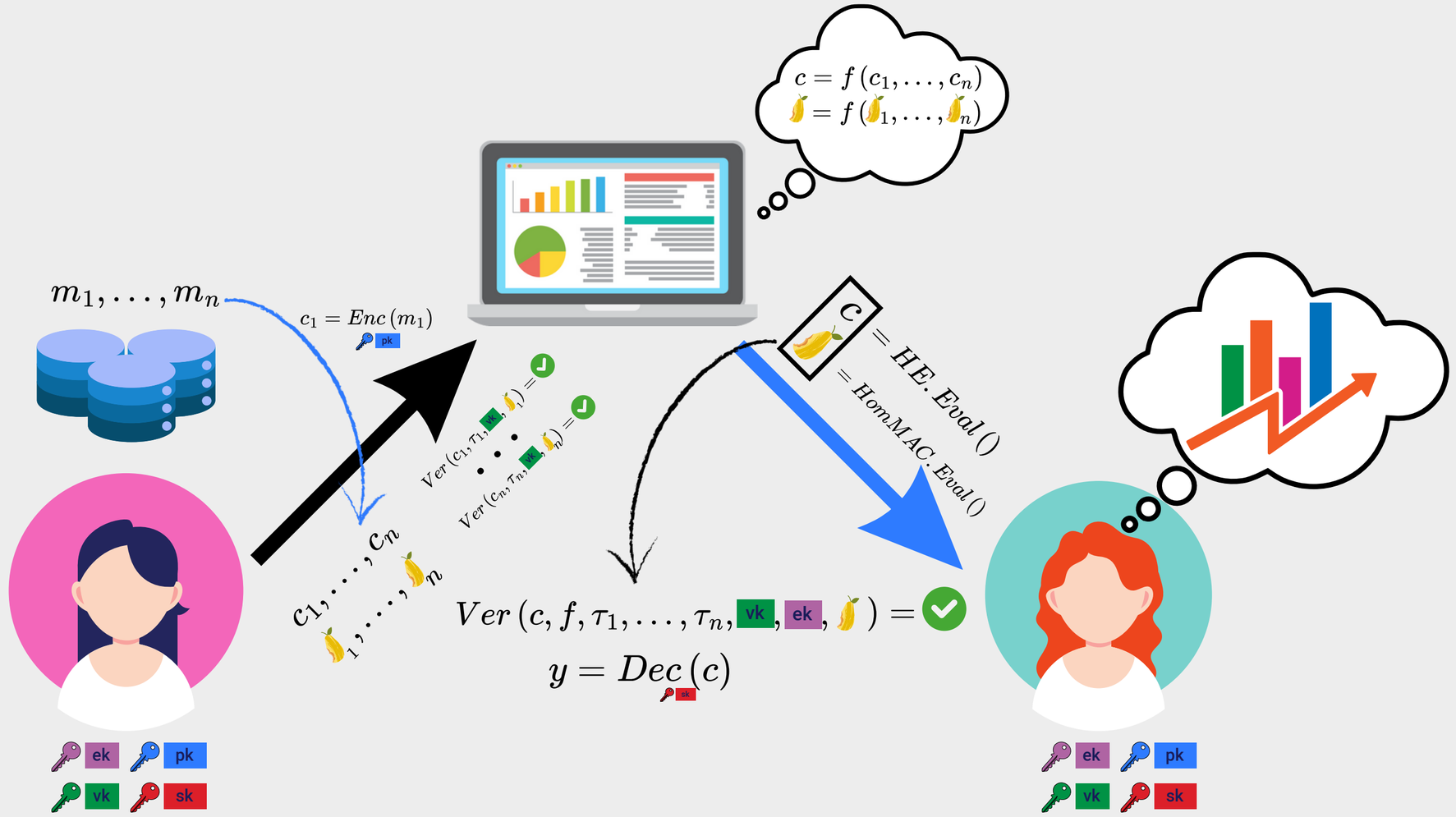
CF13: $Z_q \mapsto Z_q^2$

Solucionado:

- **PRIVACIDAD:** Encriptamos homomórficamente los datos.



EL PROTOCOLO DE CV SEGURO



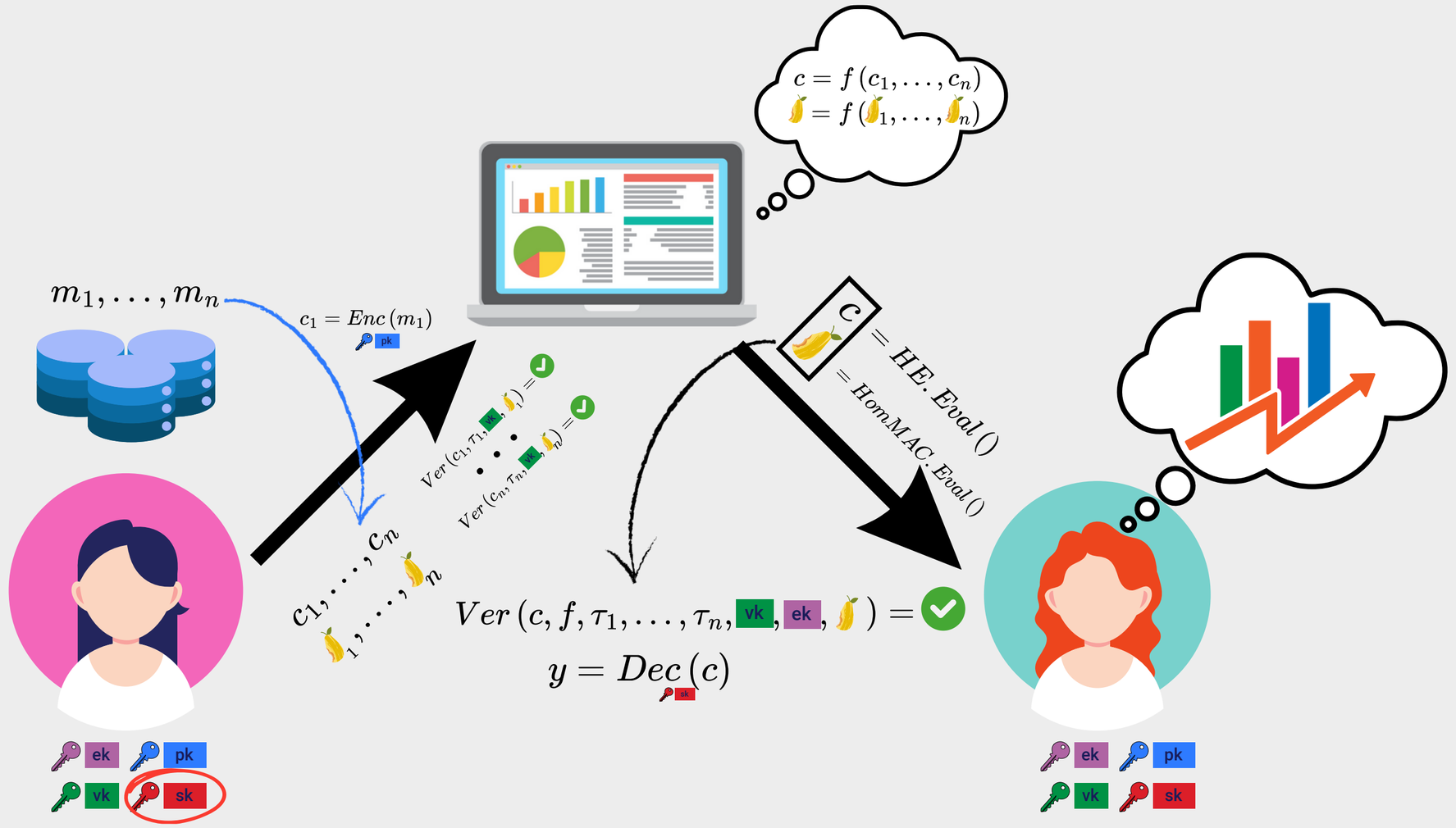
BV11: $R_t \mapsto R_q^2$

CF13: $Z_q \mapsto Z_q^2$

Solucionado:

- **PRIVACIDAD:** Encriptamos homomórficamente los datos.
- **FALSABILIDAD:** Ahora es posible saber si los resultados que (📊) envía son honestos.

EL PROTOCOLO DE CV SEGURO



BV11: $R_t \mapsto R_q^2$

CF13: $Z_q \mapsto Z_q^2$

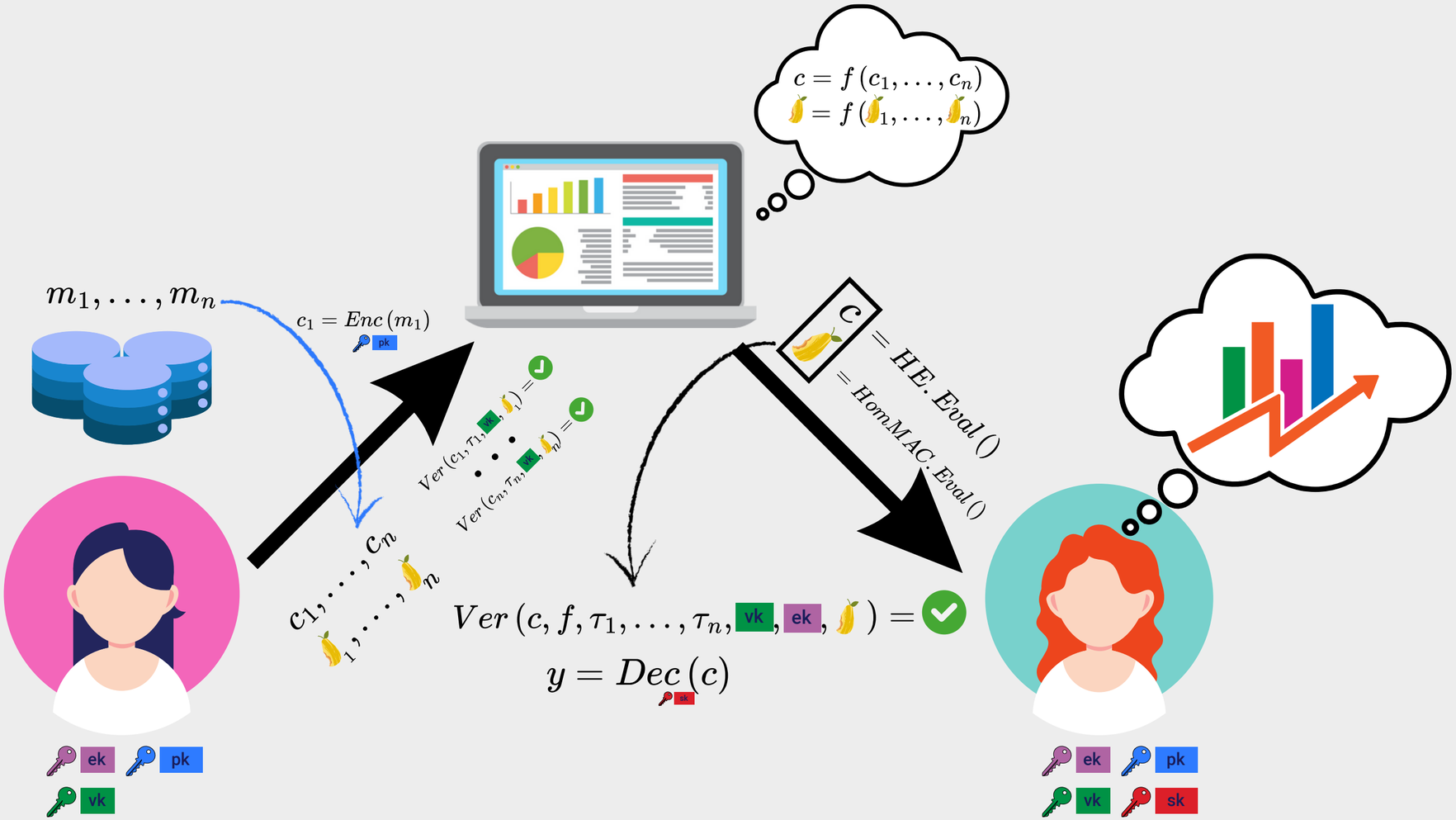
Solucionado:

- **PRIVACIDAD:** Encriptamos homomórficamente los datos.
- **FALSABILIDAD:** Ahora es posible saber si los resultados que (💻) envía son honestos.

EL PROTOCOLO DE CV MEJORADO

$\mathbf{BV11}: R_t \mapsto R_q^2$

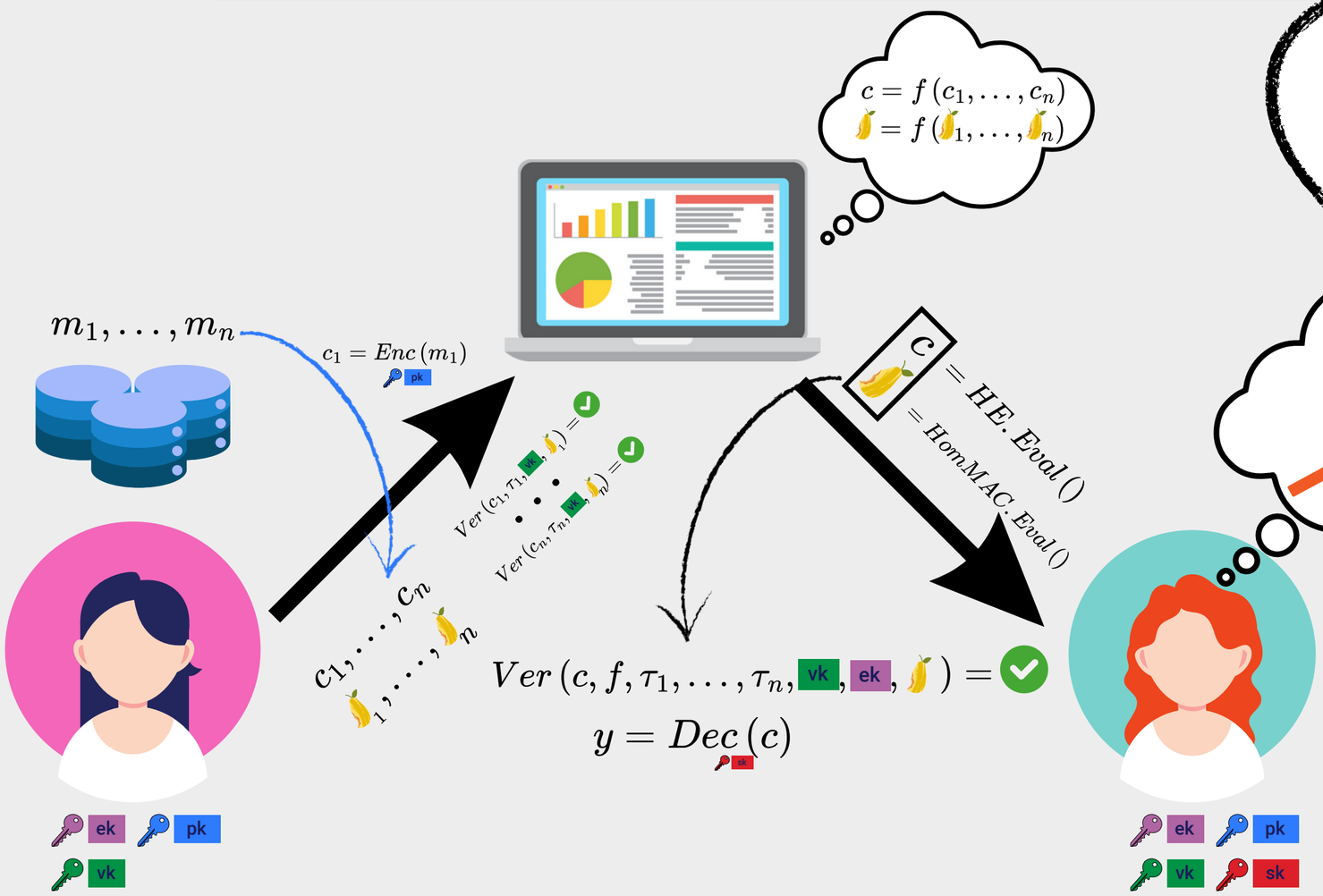
$\mathbf{\widetilde{CF13}}: R_q \mapsto R_q^2$



Solucionado:

- **PRIVACIDAD:** Encriptamos homomórficamente los datos.
- **FALSABILIDAD:** Ahora es posible saber si los resultados que (🖥) envía son honestos.

EL PROTOCOLO DE CV MEJORADO



En el PFM probamos formalmente que CF13 es seguro y funciona. Por tanto, el esquema global es seguro.

BV11: $R_t \mapsto R_q^2$

CF13: $R_q \mapsto R_q^2$

Solucionado:

PRIVACIDAD: Encriptamos homomórficamente los datos.

- **FALSABILIDAD:** Ahora es posible saber si los resultados que (🖥) envía son honestos.

CONCLUSIONES

CONCLUSIONES

Conseguimos un sistema de Computación Verificable seguro, eficiente y correcto.

CONCLUSIONES

Conseguimos un sistema de Computación Verificable seguro, eficiente y correcto.

Puede enviar sus datos sin exponerlos gracias a la encriptación.

CONCLUSIONES

Conseguimos un sistema de Computación Verificable seguro, eficiente y correcto.

Puede enviar sus datos sin exponerlos gracias a la encriptación.

Obtiene los resultados que quería sabiendo que provienen del emisor correcto.

CONCLUSIONES

Conseguimos un sistema de Computación Verificable seguro, eficiente y correcto.

Puede enviar sus datos sin exponerlos gracias a la encriptación.

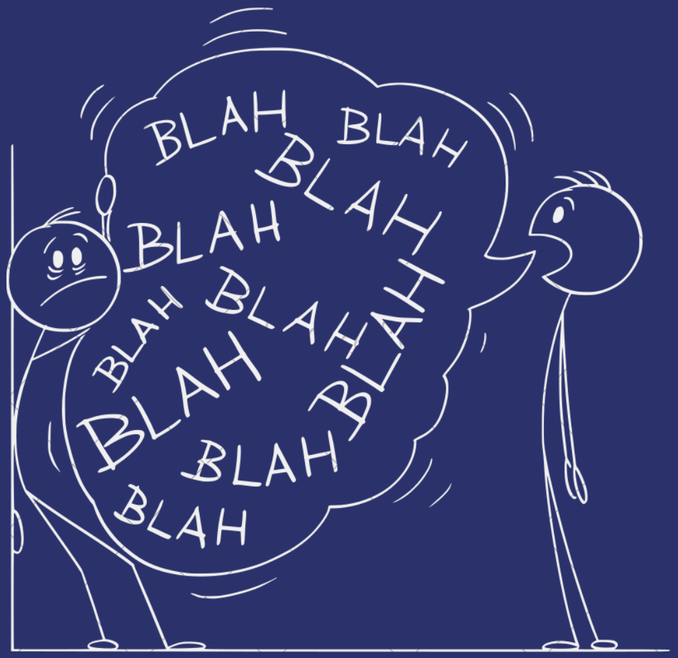
Obtiene los resultados que quería sabiendo que provienen del emisor correcto.

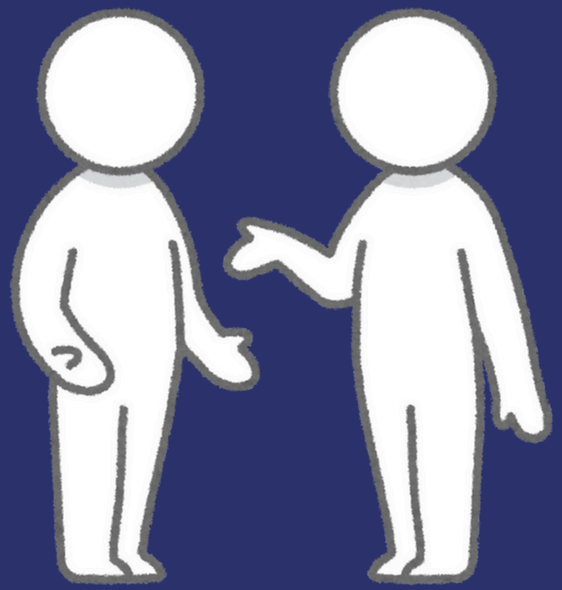
No puede engañar en el protocolo gracias a la seguridad del MAC.

TRABAJO FUTURO

En el PFM conseguimos un sistema de CV eficiente en términos de complejidad de comunicación. Sin embargo, puede ser mejorado con técnicas vistas en trabajos como [6] usando *Homomorphic Hashes*.

[6] Bois, A., Cascudo, I., Fiore, D., & Kim, D. (2021, May). Flexible and efficient verifiable computation on encrypted data. In IACR International Conference on Public-Key Cryptography (pp. 528-558). Cham: Springer International Publishing.





REFERENCIAS

[1] Gennaro, R., Gentry, C., & Parno, B. (2010). Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In Advances in Cryptology–CRYPTO 2010: 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings 30 (pp. 465-482). Springer Berlin Heidelberg.

[2] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[3] Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 56(6), 1-40.

[4] Brakerski, Z., & Vaikuntanathan, V. (2011, August). Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Annual cryptology conference (pp. 505-524). Berlin, Heidelberg: Springer Berlin Heidelberg.

[5] Catalano, D., & Fiore, D. (2013, May). Practical homomorphic MACs for arithmetic circuits. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 336-352). Berlin, Heidelberg: Springer Berlin Heidelberg.

[6] Bois, A., Cascudo, I., Fiore, D., & Kim, D. (2021, May). Flexible and efficient verifiable computation on encrypted data. In IACR International Conference on Public-Key Cryptography (pp. 528-558). Cham: Springer International Publishing.

MUCHAS GRACIAS

¿Preguntas?