PhotoLock

•••

Chino Cribioli, Caro Lang, Lorenzo Ruiz Díaz, Bruno Weisz

Resumen

PhotoLock es una herramienta que permite generar y verificar pruebas de veracidad sobre imagenes editadas.

Permite, mediante Zero-Knowledge Proofs, demostrar y/o verificar a un agente que una foto viene del lugar del cual afirma venir.

Somos como Photoshop, pero con ZK.

Vivimos en la era de la (des)información

Los rápidos avances en la tecnología de la Inteligencia Artificial han permitido que estas generen cantidades impresionantes de información, muchas veces falsa.

Pero no todo está perdido... ¡la solución la brinda la criptografía!

¿Qué se puede hacer hoy?

Supongamos que un diario tiene una foto la cual fue capturada con una cámara que tiene una clave privada integrada (a la cual no tenemos acceso) que usa para firmar digitalmente cada foto que toma junto con cierta Metadata, como fecha, hora y lugar.

Entonces, dada la clave pública del dispositivo y la firma digital de cierto par Foto-Metadata, actualmente es posible verificar si la foto que vemos fue efectivamente sacada en el momento y lugar que el diario afirma.

¿Pero y si la foto es transformada...?

¿Qué se puede hacer hoy?

Supongamos que un diario tiene una foto la cual fue capturada con una cámara que tiene una clave privada integrada (a la cual no tenemos acceso) que usa para firmar digitalmente cada foto que toma junto con cierta Metadata, como fecha, hora y lugar.

Entonces, dada la clave pública del dispositivo y la firma digital de cierto par Foto-Metadata, actualmente es posible verificar si la foto que vemos fue efectivamente sacada en el momento y lugar que el diario afirma.

¿Pero y si la foto es transformada...?

Acá está la solución.

Garantizar Propiedades de Seguridad en las Transformaciones

PhotoLock es una herramienta que al realizar una transformación (o composición de transformaciones) sobre una foto genera una prueba criptográfica de que el resultado es producto de estas transformaciones válidas, siempre **sobre una imagen firmada correctamente** .

En este caso, a pesar de que la firma ya no es válida para la foto resultante, se puede verificar su veracidad mediante una ZKP.

Ejemplo de recorte de una fotografía del Aconcagua.

Imagen con una firma válida.

PhotoLock: Generación de una prueba verificable.

PhotoLock

Nuestro producto estará compuesto por:

- Una Aplicación Web para publicar fotos verificadas.
- Una extensión del navegador para verificar una foto.

Más aún, gracias a la tecnología de zkSNARK, la verificación es sumamente rápida y por ende es un proceso muy democrático.

Solamente con una billetera de Ethereum, ¡el usuario puede verificar el origen de la foto por su cuenta!

PhotoLock

Ubicación: XXXX
Fecha: XX/XX/XX

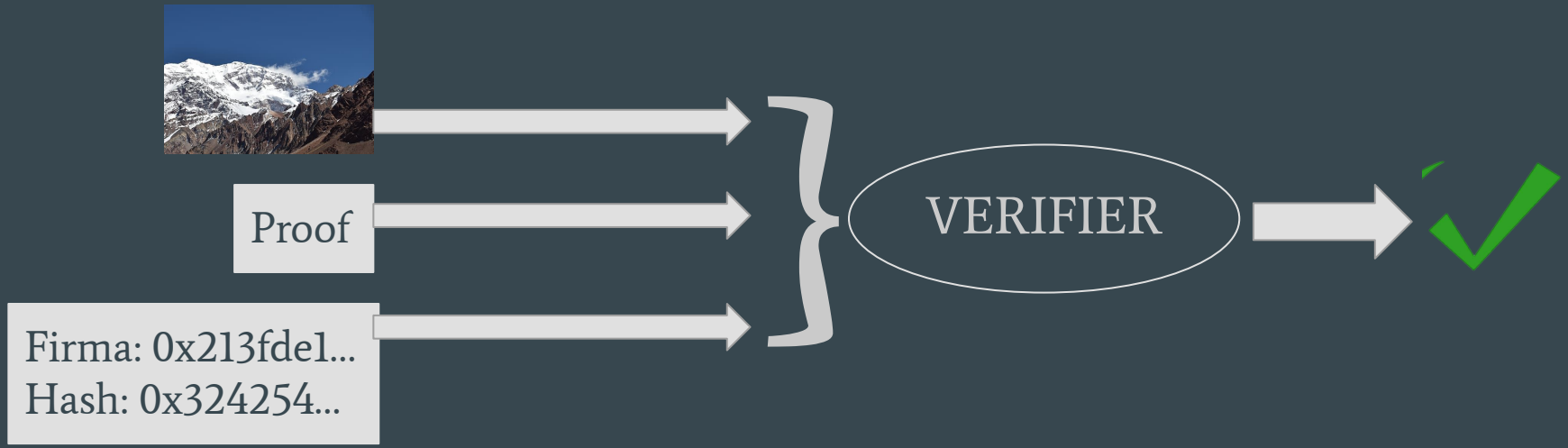
Firma: 0x213fde1...
Hash: 0x324254...

Transformaciones:
Recorte(offset, dimensiones)

PROVER

Proof

PhotoLock



Público Objetivo

PhotoLock apunta principalmente a ser utilizada por:

- Diarios digitales. Ahora, podrán recortar las imágenes a conveniencia y adjuntar una prueba de que no están falsificadas ni manipuladas maliciosamente.
- Lectores escépticos. ¡Hoy más que nunca es relevante ser escéptico! Incluso idealmente sería posible exigir estas pruebas a los diarios.

Se genera una sinergia entre ambos grupos, que le gana a la desconfianza.

Trabajo Futuro

La aplicación funciona actualmente para la operación de recorte de fotos. Queremos:

- Más transformaciones, como homotecias, rotaciones, recortes no cuadrados.
- Aplicar la composición de transformaciones de diferentes tipos.
- Aumentar el tamaño máximo de imagen permitida.

¡Muchas gracias!