Ataques diversos

Criptografía cuántica

Principios, herramientas y protocolos de criptografía

Yann Frauel – Semestre 2007-1

1. Ataques

Ataques contra claves

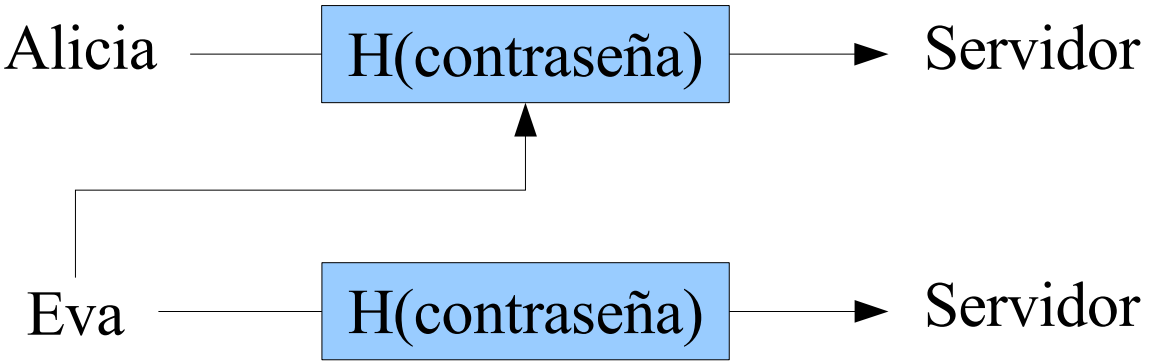
- Adivinar la clave (usando contraseñas comunes, datos personales)
- Ataque de diccionario
- Factorización, logaritmo discreto (claves públicas)
- Ataque por fuerza bruta (búsqueda exhaustiva)

Ataques contra algoritmos

- Texto cifrado sólo
- Texto claro conocido (ej. cripto. lineal)
- Texto claro escogido (ej. cripto. diferencial)
- Texto claro escogido adaptativo
- Texto cifrado escogido
- Texto cifrado escogido adaptativo

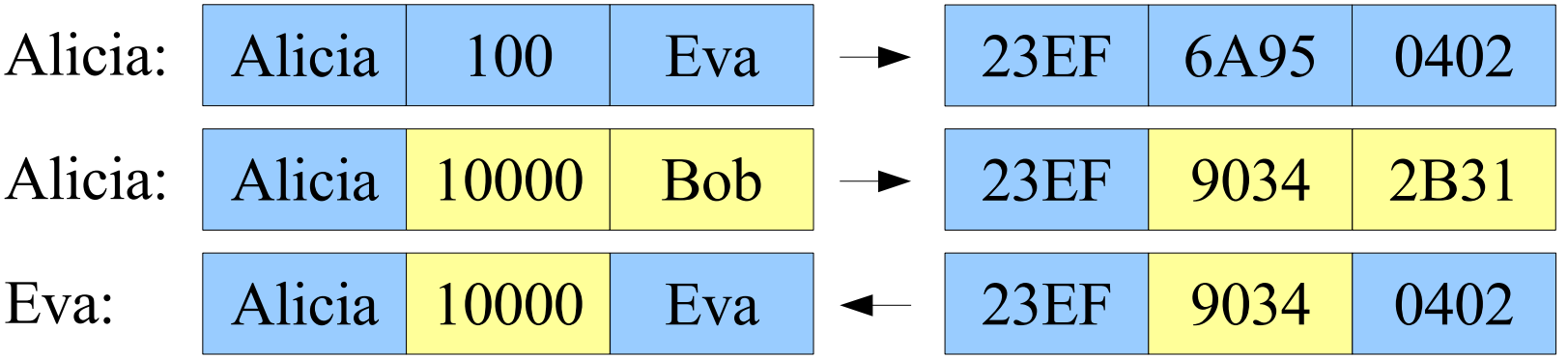
Ataques contra protocolos (1)

- Ataque de repetición (replay attack)
  - ➔ Ej. 1: Autenticación usuario/servidor



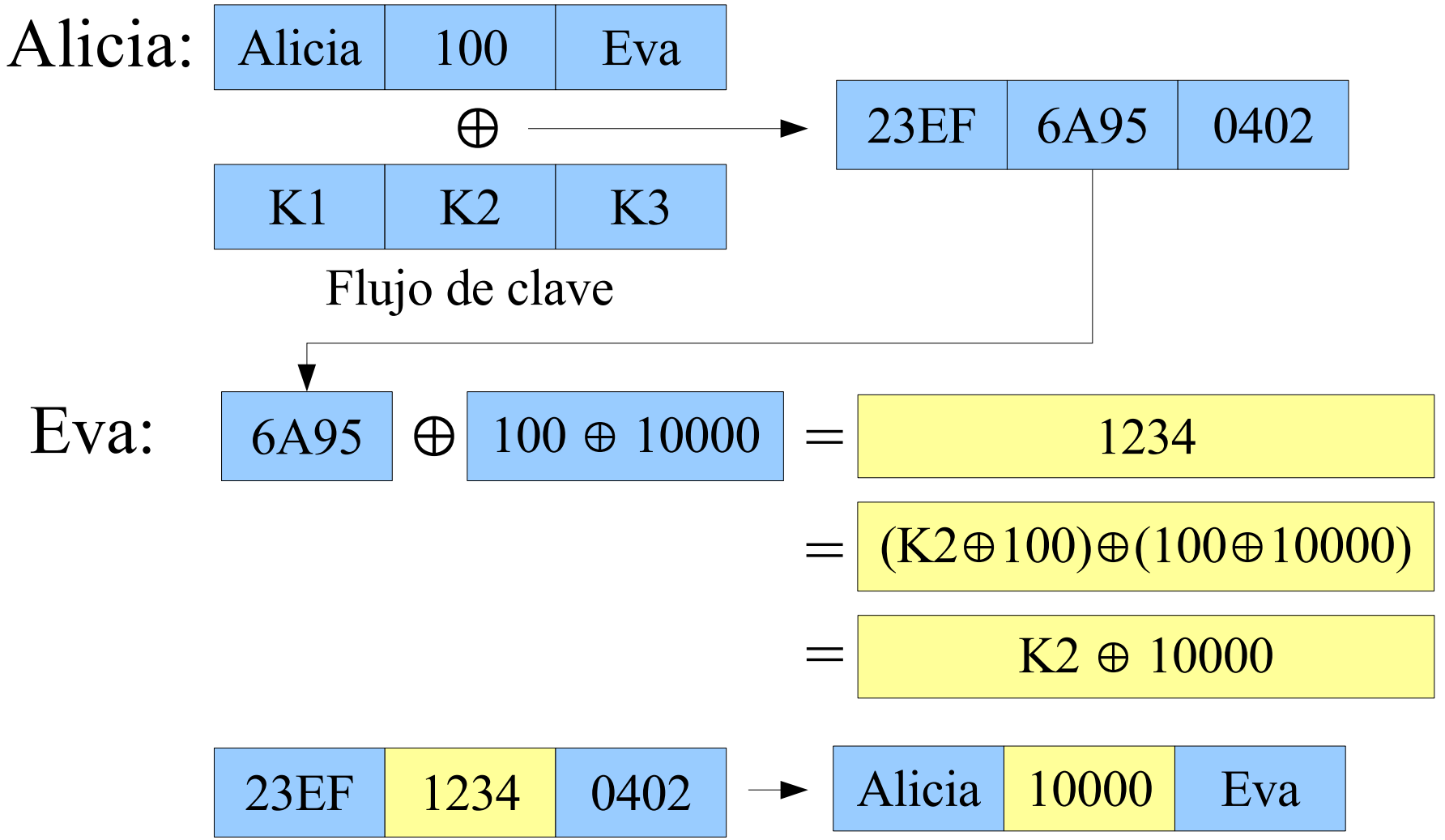
  - ➔ Ej. 2: orden de traspaso bancario (cifrado de bloque, ECB)

    Formato: (cuenta origen, cantidad, cuenta destinación)



Ataques contra protocolos (2)

- Ataque de substitución
  - ➔ Ej.: orden de traspaso bancario (cifrado de flujo)



Ataques contra protocolos (3)

- Ataque de diccionario (contra contraseñas)
- Búsqueda hacia adelante (forward search)
  - ➔ Ej.: Número de cuenta de 10 dígitos cifrado con una clave pública

    Atacante cifra todos los valores posibles hasta encontrar el texto cifrado: $10^{10} \sim 2^{33}$ intentos
- Ataque temporal (timing attack)
  - ➔ Deducir información del tiempo necesario para operaciones

Ataques contra protocolos (4)

- Suplantación (impersonation)
  - ➔ hombre-en-el-medio
  - ➔ spoofing: usar un identificador falsificado (dirección IP, MAC, de correo...)
  - ➔ phishing: obtener información de un usuario por engaño (ej. correos de Banamex)

Otros ataques

- Sniffing: escuchar comunicaciones no cifradas
- Errores de programación (Ej. desbordamiento de búfer)
- Viruses y gusanos
- Grabador de teclado
- Información dejada en el disco por la memoria virtual
- Radiación electromagnética (tempest)

El factor humano

- Errores humanos
  - ➔ Encripción parcial
  - ➔ Encripción doble con diferentes claves o algoritmos
- Pereza: si difícil de aplicar, no aplicado
- Ingeniería social (social engineering)
  - ➔ Engañar
  - ➔ Comprar
  - ➔ Amenazar
  - ➔ Chantajear

→ ¡El humano es el punto más débil!

2. Criptografía cuántica: Algoritmo BB84

Criptografía cuántica

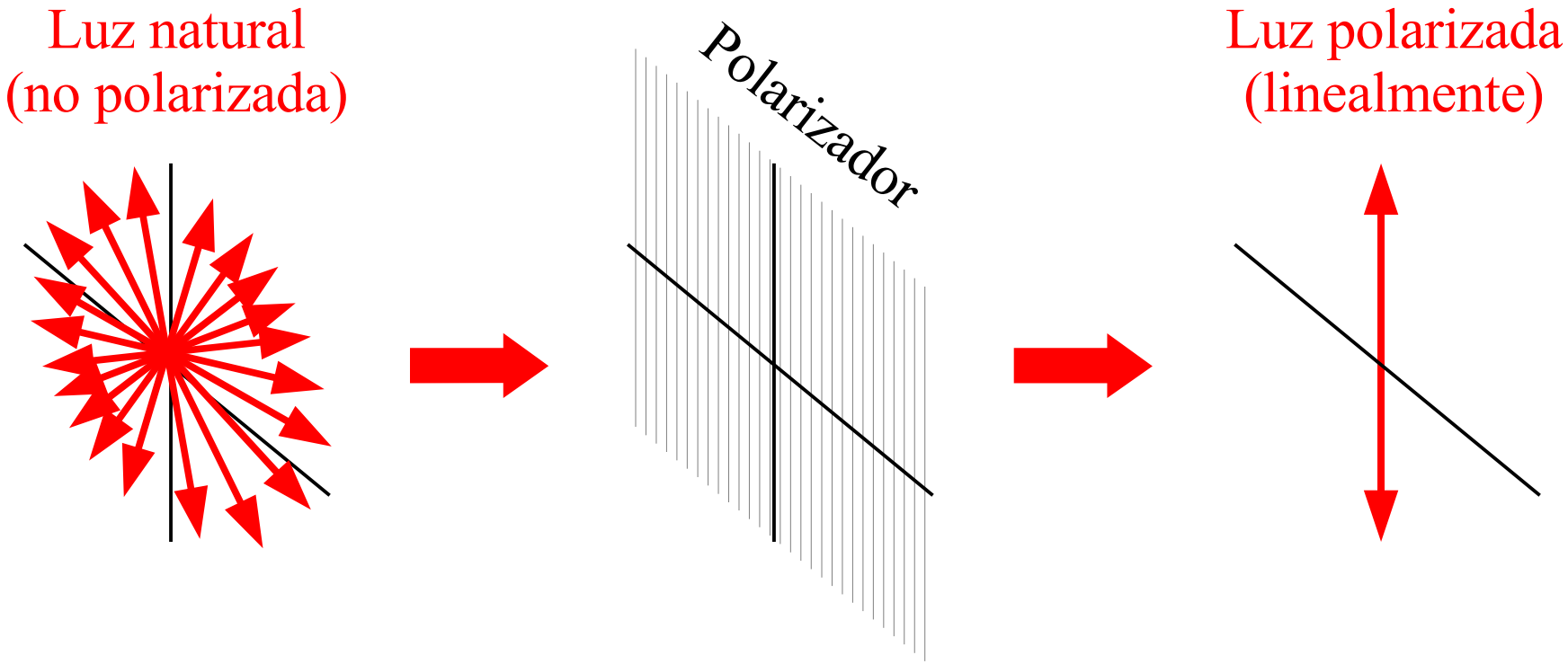
- Único algoritmo perfecto: máscara desechable
- Problema: establecer la clave común
- No existen algoritmos de encripción cuánticos, sino técnicas de intercambio de clave cuánticas
  - ➔ Bennett y Brassard 1984
  - ➔ Ekert 1991
- Permite a Alicia y Bob establecer una clave común a distancia, sin que un atacante la pueda conocer

Criptografía cuántica

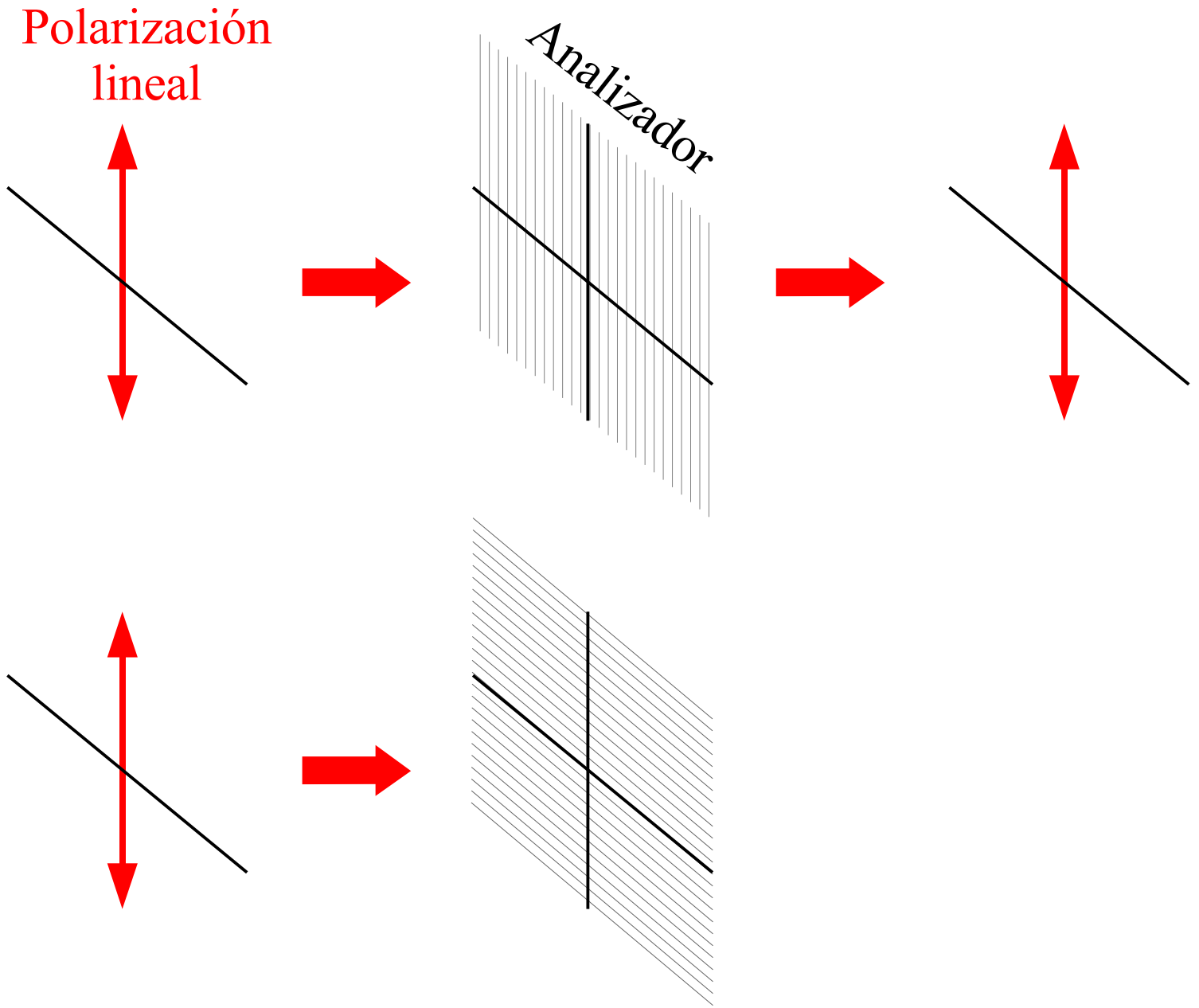
- No basado matemáticas, sino en propiedades físicas
- La seguridad no proviene de una limitación tecnológica, sino de una ley física
- Principio: el acto de medir modifica el estado del sistema estudiado
  - ➔ Si un atacante (Eva) espía la comunicación, los datos son modificados
- Usar fotones transmitidos por fibras ópticas

Polarización 1

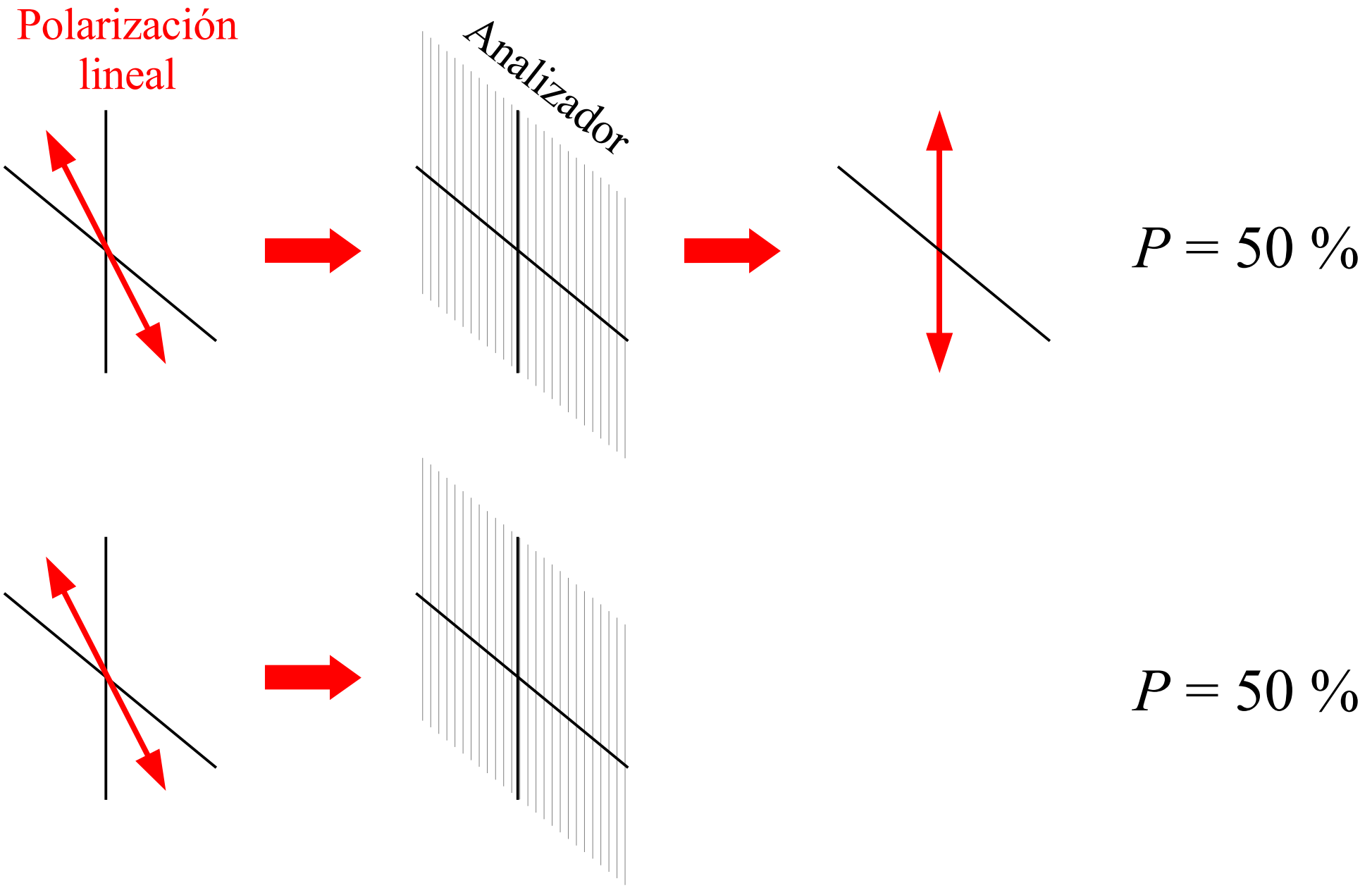
- La luz es un campo electro-magnético oscilante
- Un fotón es una unidad (cuanto) de luz
- En luz natural, la dirección de vibración del campo eléctrico de cada fotón es aleatoria



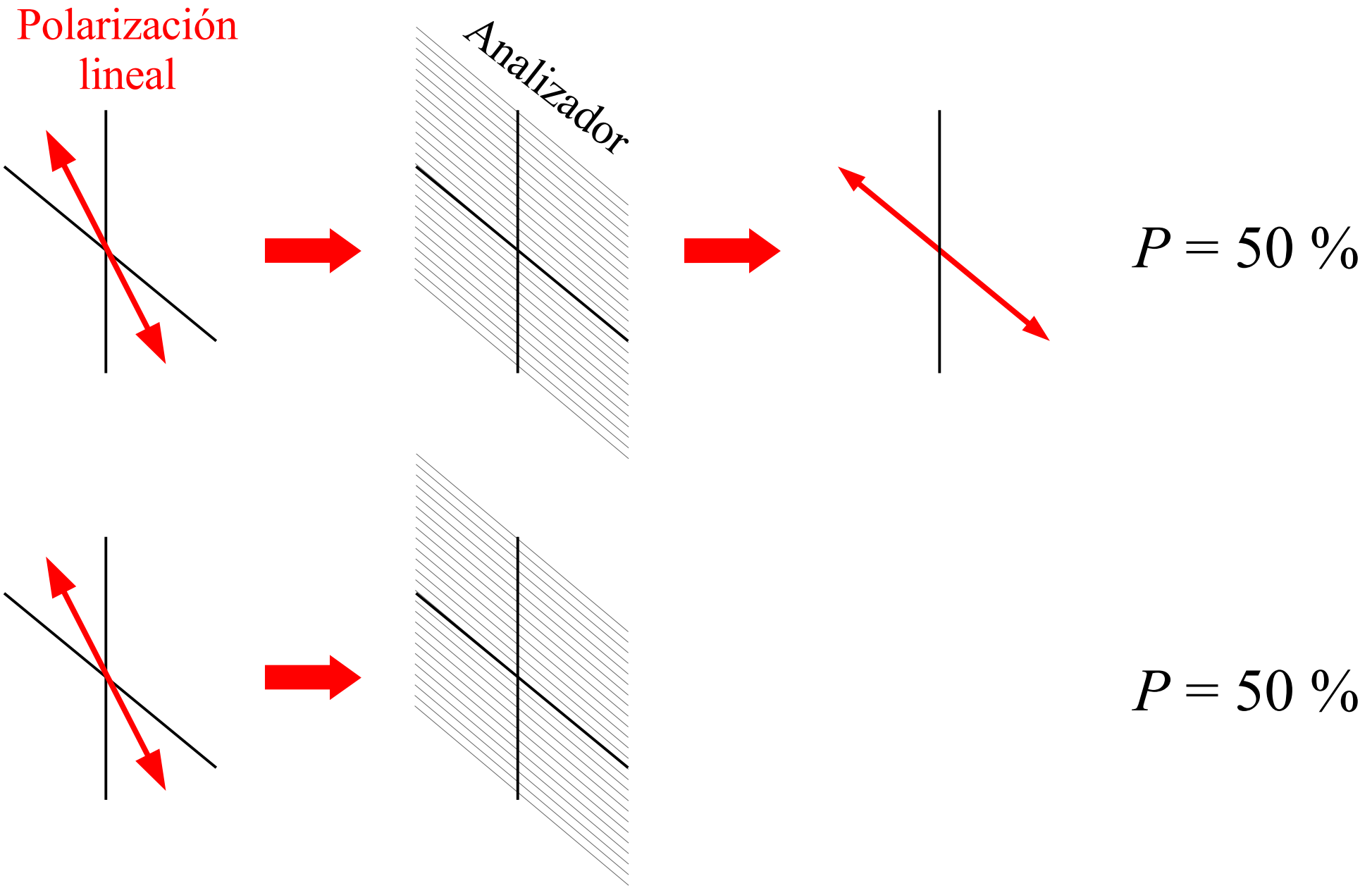
Polarización 2



Polarización 3



Polarización 4

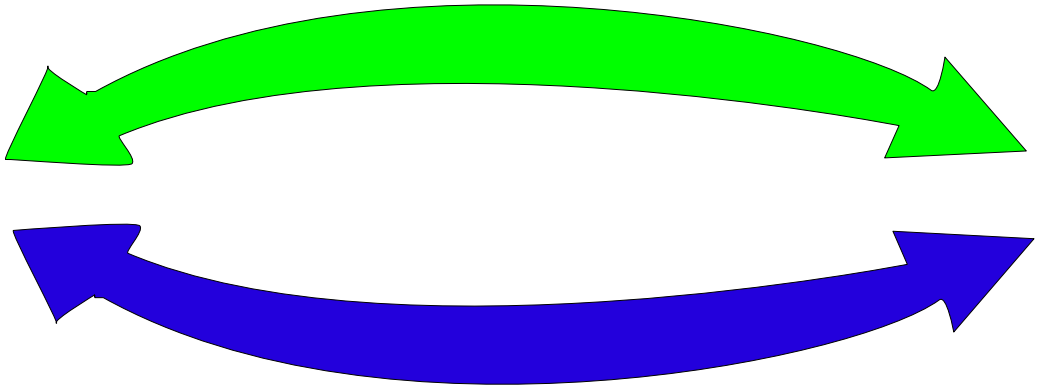


Polarización 5

- Dos bases posibles:
  - ➔ Recta (+): ejes horizontal y vertical
  - ➔ Diagonal (×): ejes a 45 grados
- El emisor escoge una base para el polarizador y escoge una polarización según uno de los dos ejes
- El receptor escoge una base para el analizador:
  - ➔ Si las bases son iguales, la medida es segura y revela la polarización emitida
  - ➔ Si las bases son diferentes, la medida es aleatoria y no revela la polarización emitida

Intercambio de clave cuántico

Canal cuántico
(fibra óptica)



Alicia

Bob

Canal clásico no modificable
(radio...)

Intercambio de clave en ausencia de Eva

Bit Alicia	0	1	1	0	0	1	0	0
Envío Alicia	-	|	/	-	\	/	\	\
Base Bob	+	+	+	X	X	X	+	+
Medida Bob	-	|	|	/	\	/	-	|
Bit Bob	0	1	1	1	0	1	0	1
Clave secreta	0	1			0	1		

- A y B escogen sus bases independientemente
- 50 % de tener bases iguales (→ bits iguales)
- Después de transmitir los bits, A y B revelan sus bases y se descartan los bits con bases diferentes

Intercambio de clave en presencia de Eva

Bit Alicia	0	1	1	0	0	1	0	0
Envío Alicia	-	|	/	-	\	/	\	\
Base Eva	+	X	X	+	+	X	+	+
Medida Eva	-	/	/	-	|	/	-	|
Bit Eva	0	1	1	0	1	1	0	1
Base Bob	+	+	+	X	X	X	+	+
Medida Bob	-	-	|	/	\	/	-	|
Bit Bob	0	0	1	1	0	1	0	1
Clave Alicia	0	1			0	1		
Clave Eva	0	1			1	1		
Clave Bob	0	0			0	1		

- Eva se equivoca de base en 50% de los casos
- Con una base equivocada, tiene 50% de medir un bit equivocado y 50% que B reciba un bit equivocado

Detección de Eva

- Alicia y Bob revelan (y descartan) una fracción de los bits
- Si Eva está presente, habrá introducido errores
- Eva puede escuchar parcialmente para reducir la tasa de errores
- En práctica, no se puede saber si los errores provienen de Eva o de la comunicación imperfecta

Finalización del protocolo

- Reconciliación: Alicia y Bob eliminan los bits erróneos revelando la paridad de bloques
  - ➔ En este punto, Alicia y Bob tienen bits comunes parcialmente conocidos por Eva
- Amplificación de secreto: Alicia y Bob aplican una técnica de hash a sus bits
  - ➔ Con su información incompleta, Eva no puede calcular el hash
  - ➔ Entonces Alicia y Bob tienen una secuencia de bits comunes desconocida por Eva

Ventajas/desventajas

- Seguridad absoluta
- Caro y difícil (equipo especializado)
- Fase de desarrollo
- Demostración hasta 50 km
- Considerado para comunicaciones por satélite