A Few Notions in Cryptography

Palash Sarkar

Applied Statistics Unit
Indian Statistical Institute, Kolkata
India
palash@isical.ac.in

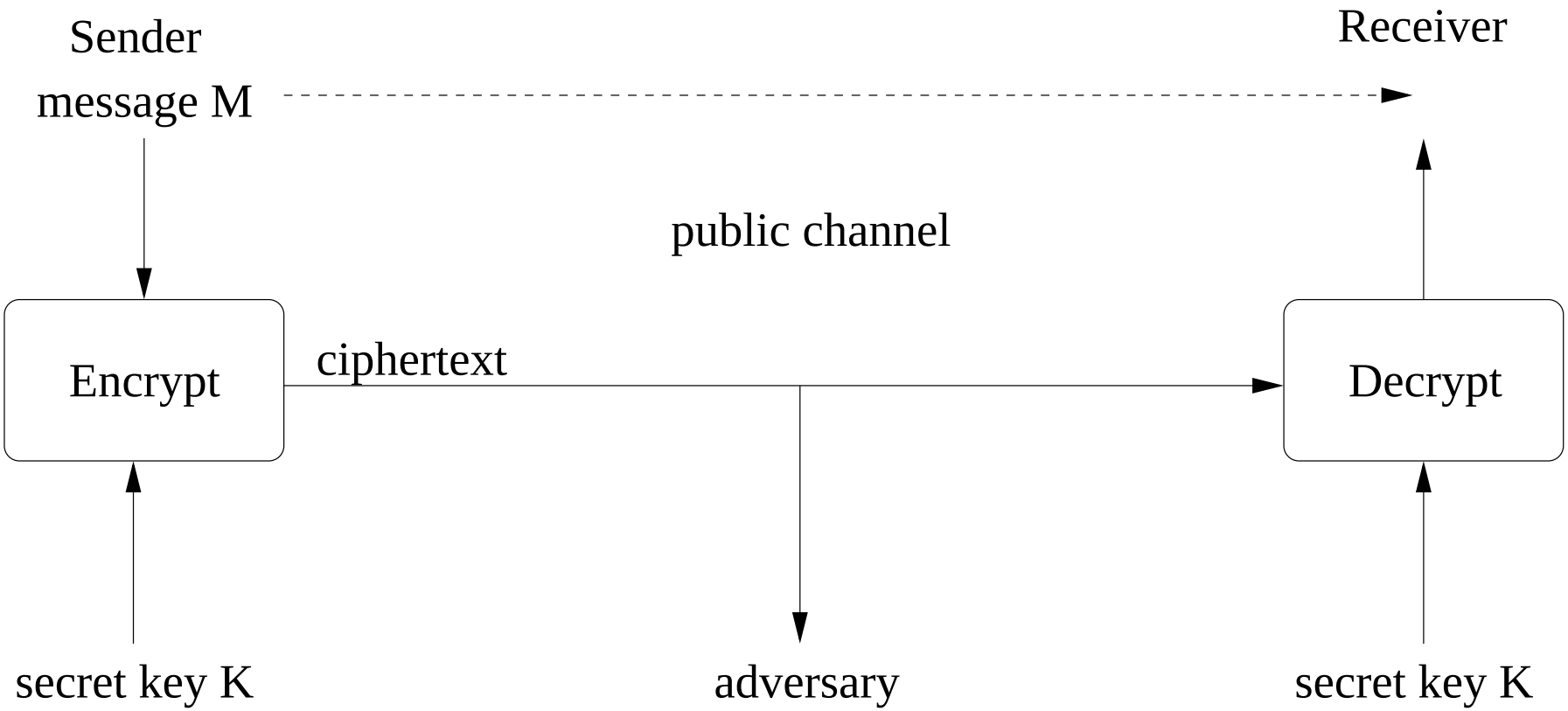
Madras Christian College,
26th June 2010



Classical Symmetric Key Encryption



Introduction

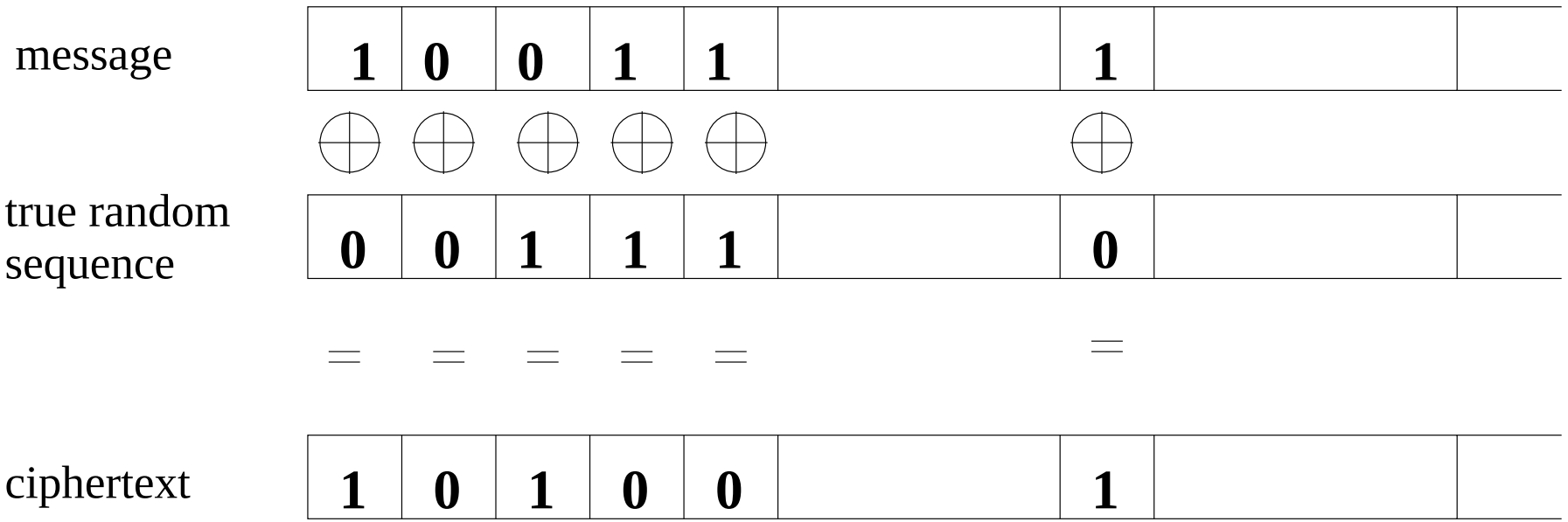


Attack Models

- **Ciphertext only attack:**
  the attacker has access to only ciphertext(s);
  goal: find (one of) the message(s) and/or the key.
- **Known plaintext attack:**
  the attacker *knows* $(P_1, C_1), \ldots, (P_t, C_t)$;
  goal: find the key or find P^* corresponding to a "new" C^*.
- **Chosen plaintext attack:**
  the attacker *chooses* $P_1, \ldots, P_t$;
  receives corresponding $C_1, \ldots, C_t$;
  goal: find the key or find P^* corresponding to a "new" C^*.
- **Chosen ciphertext attack.**



One-Time Pad


message
1 0 0 1 1 1
true random sequence
0 0 1 1 1 0
ciphertext
1 0 1 0 0 1

Perfect Secrecy of One-Time Pad

For $a, b \in \{0, 1\}$,

$$
\begin{aligned}
\Pr[M_i = a | C_i = b] &= \frac{\Pr[M_i = a \wedge C_i = b]}{\Pr[C_i = b]} \\
&= \frac{\Pr[M_i = a, M_i \oplus K_i = b]}{\Pr[M_i \oplus K_i = b]} \\
&= \frac{\Pr[M_i = a, K_i = a \oplus b]}{\Pr[M_i = 0, K_i = b] + \Pr[M_i = 1, K_i = 1 \oplus b]} \\
&= \frac{\Pr[M_i = a] \times \Pr[K_i = a \oplus b]}{\Pr[M_i = 0]\Pr[K_i = b] + \Pr[M_i = 1]\Pr[K_i = 1 \oplus b]} \\
&= \frac{\frac{1}{2}\Pr[M_i = a]}{\frac{1}{2} \times (\Pr[M_i = 0] + \Pr[M_i = 1])} \\
&= \frac{\frac{1}{2}\Pr[M_i = a]}{\frac{1}{2}} \\
&= \Pr[M_i = a].
\end{aligned}
$$



Perfect Secrecy: General Notion

Entropy. Let X be a random variable with distribution $(p_0, \ldots, p_\ell)$.

$$H(X) \stackrel{\Delta}{=} -\sum p_i \log_2 p_i.$$

Conditional entropy.

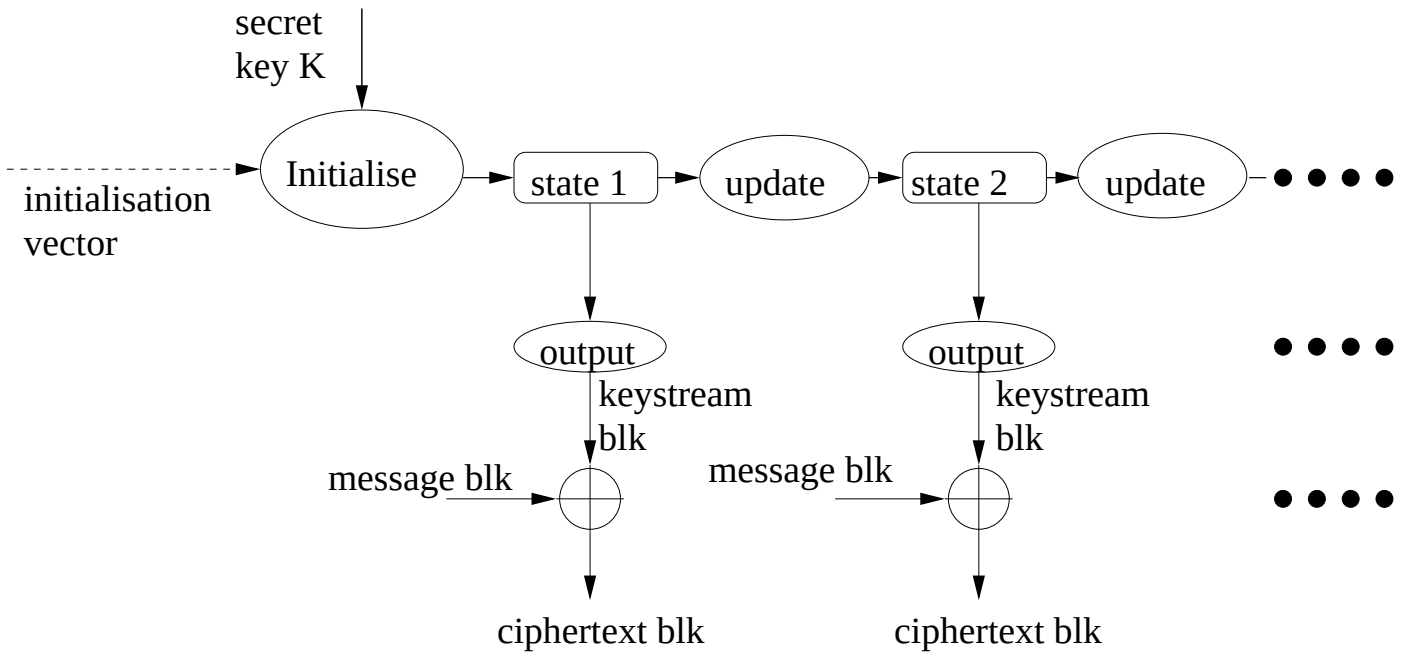
$$H(Y|X) = \Pr[X = 0]H(Y|X = 0) + \Pr[X = 1]H(Y|X = 1).$$

Perfect Secrecy.

$$H(M) = H(M|C).$$

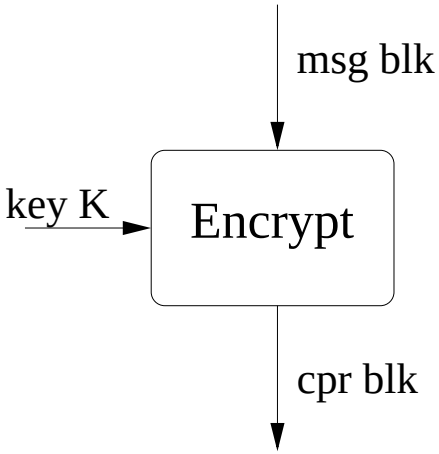


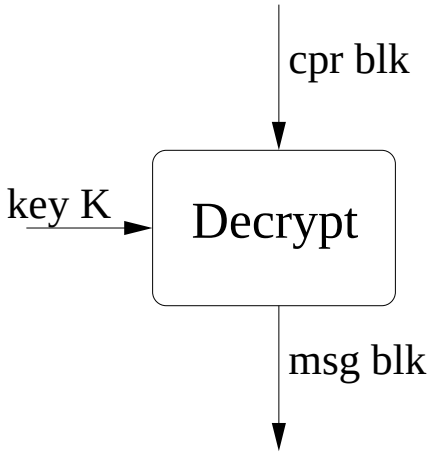
Model of Additive Stream Cipher



- Key: k bits; IV: (usually) $\leq k$ bits; state: (usually) $\geq 2k$ bits;
- initialise, update, output: functions (deterministic algorithms);
- keystream blk, msg blk, cpr blk: ≥ 1 bit.
- **Security:** keystream sequence should be computationally indistinguishable from a true random sequence.

Encrypting Short Fixed Length Strings





Block Cipher.

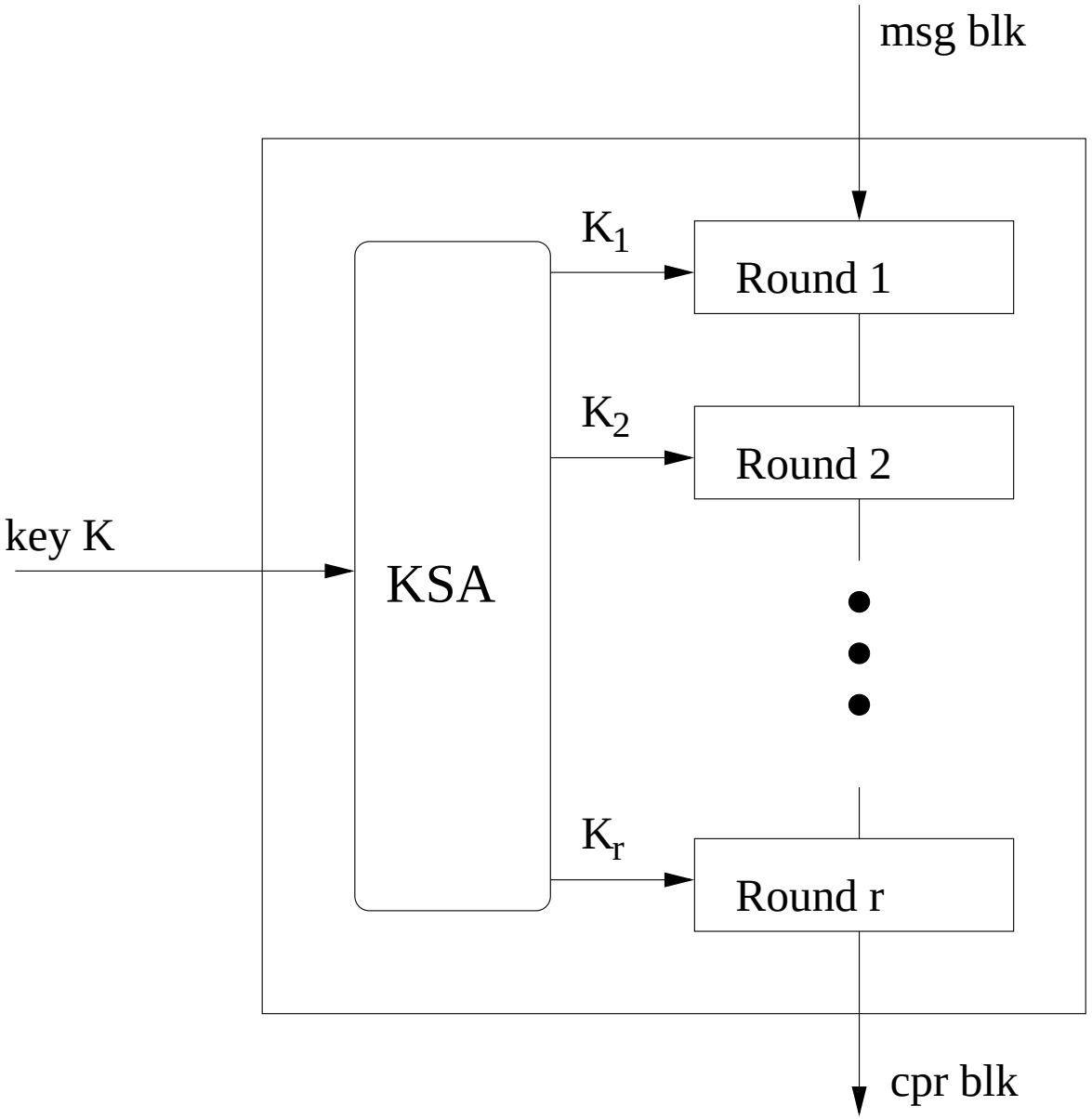
$$E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n.$$

$$D : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n.$$

For each $K \in \{0,1\}^k$,

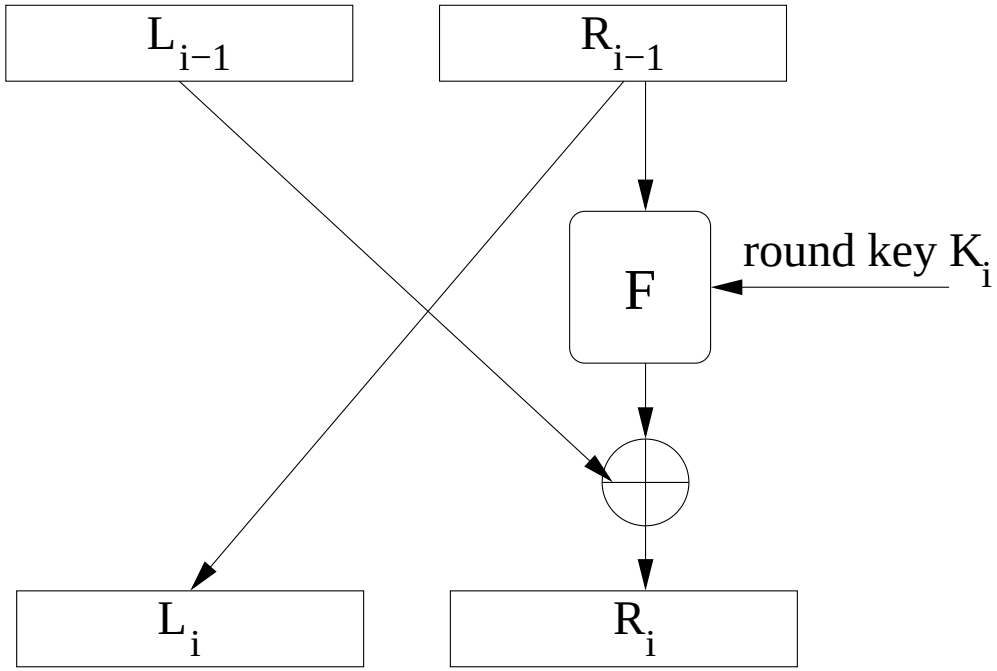
$$D_K(E_K(M)) = M.$$

Overall Structure of a Block Cipher



KSA: key scheduling algorithm

Feistel Structure

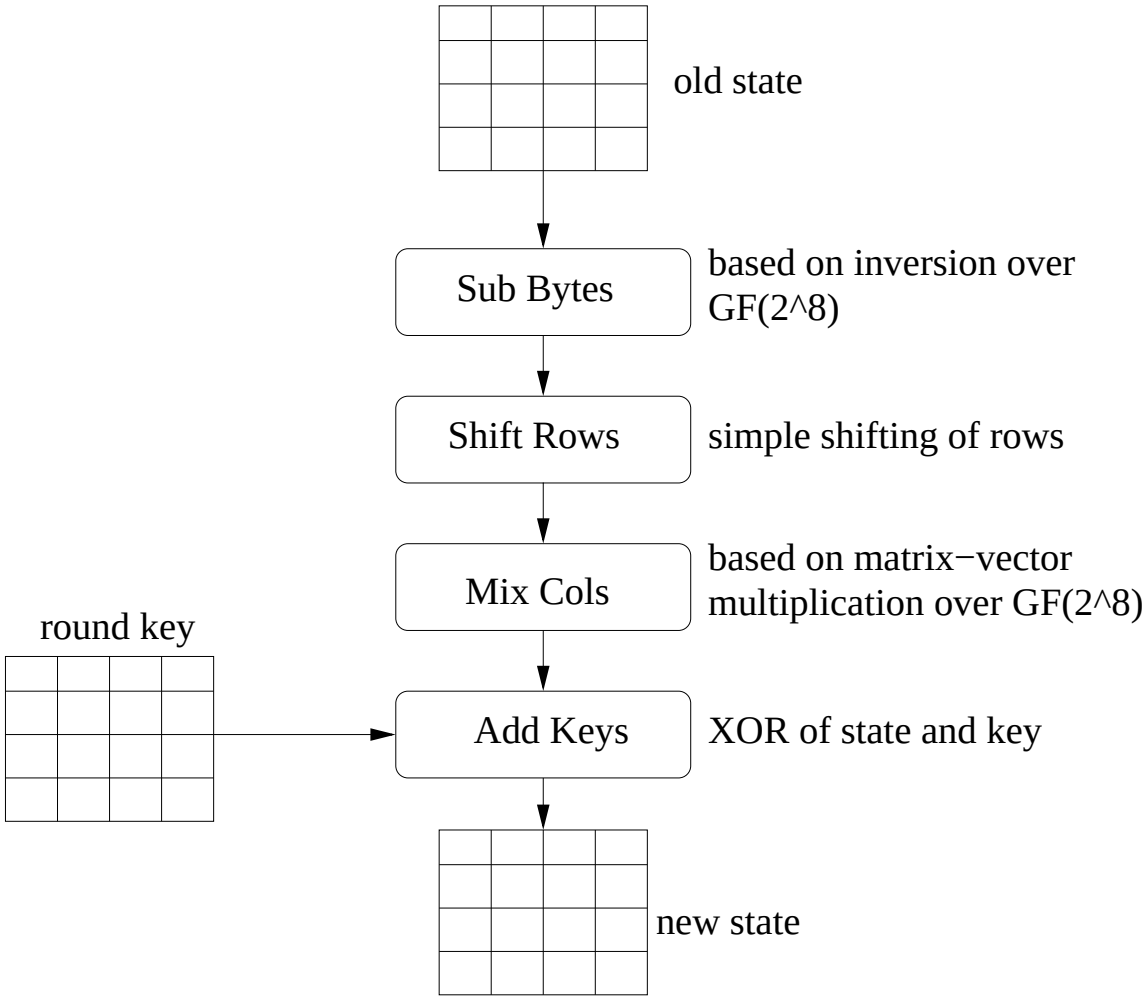


$$
\begin{aligned}
L_i &= R_{i-1}; \\
R_i &= L_{i-1} \oplus F(R_{i-1}, K_i).
\end{aligned}
$$

- Irrespective of F, the map is invertible.
- Security depends on the design of F.



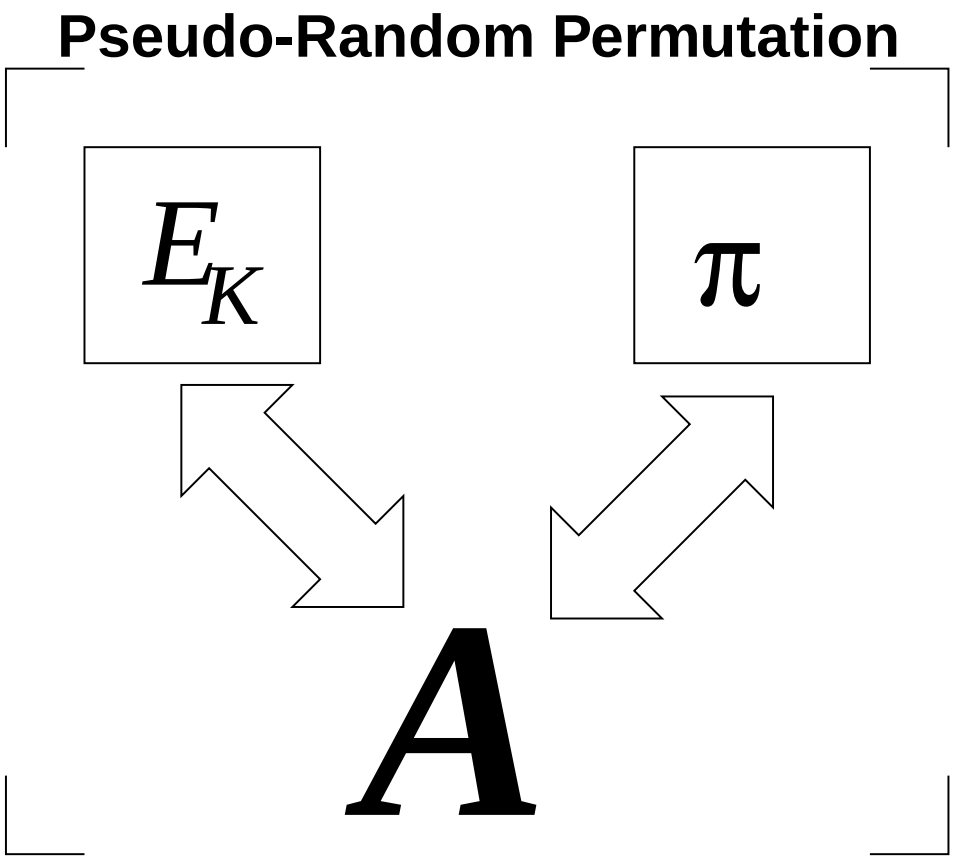
Round Structure of AES



A Bit of Formalism



Idealisation of a Block Cipher (1)

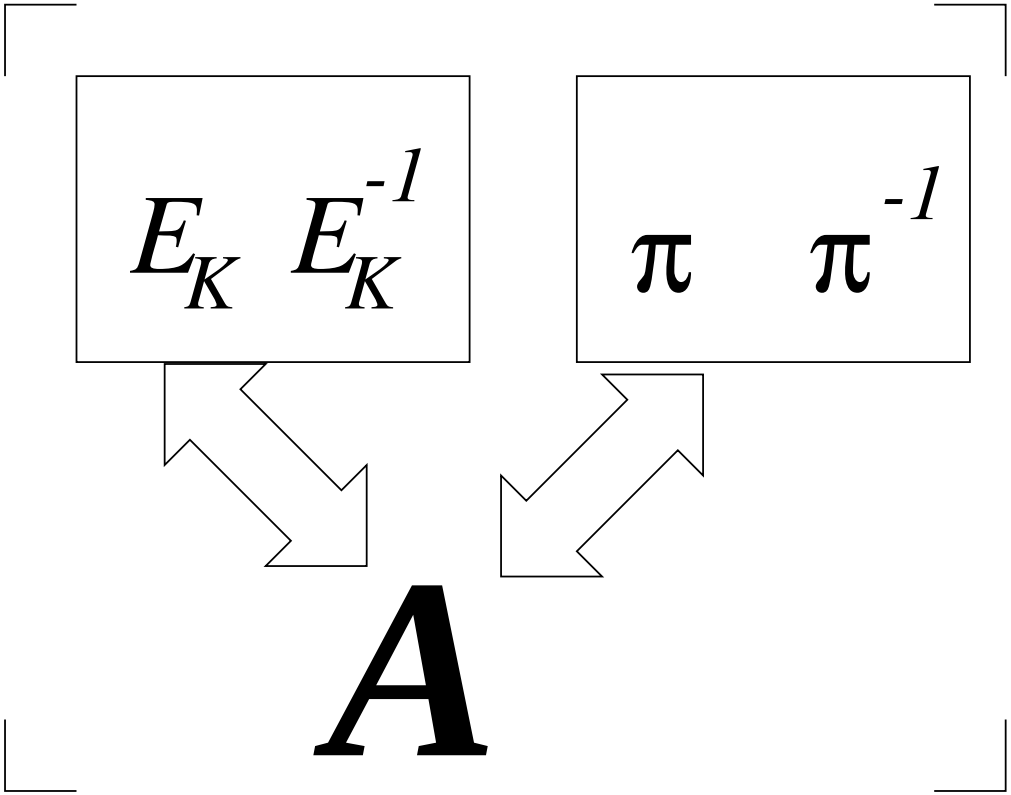


$$\mathsf{Adv}(\mathcal{A}) = |\Pr[\mathcal{A}^{E_K} \Rightarrow 1] - \Pr[\mathcal{A}^{\pi} \Rightarrow 1]|.$$



Idealisation of a Block Cipher (2)

Strong Pseudo-Random Permutation



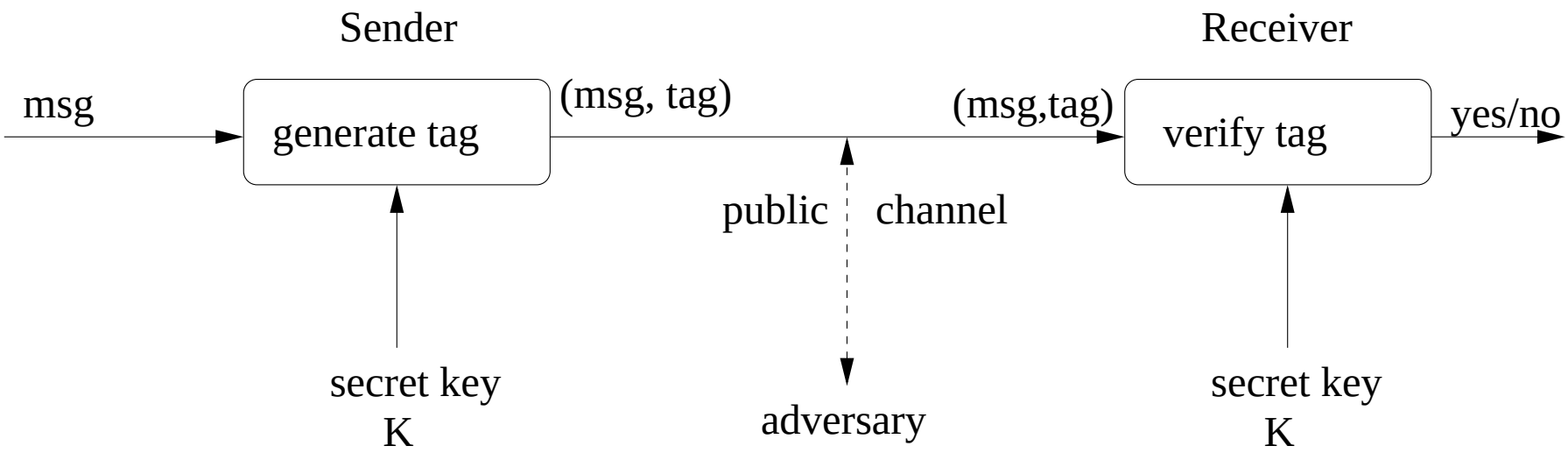
$$\mathsf{Adv}(\mathcal{A}) = |\Pr[\mathcal{A}^{E_K, E_K^{-1}} \Rightarrow 1] - \Pr[\mathcal{A}^{\pi, \pi^{-1}} \Rightarrow 1]|.$$



Authentication: The Conjoined Twin of Encryption



Authentication: General Idea



- **Active adversary:**
  - can listen to and modify information on the public channel;
  - can obtain tag corresponding to chosen messages.
- **Adversarial goal:**
  - To make the receiver accept a msg-tag pair not generated by the sender.



Authentication: A Simple Scheme

Let $\{H_\tau\}_{\tau \in \mathcal{T}}$ be a family of functions such that

- for each τ, $H_\tau : \mathcal{M} \rightarrow \{0,1\}^n$;
- for a uniform random τ, and any two distinct M_1, M_2,

$$\Pr[H_\tau(M_1) = H_\tau(M_2)] \leq \varepsilon.$$

Let $E_K : \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher.

Tag generation:

$$M \mapsto (M, \text{tag})$$

where $\text{tag} = E_K(H_\tau(M))$.



Construction of Suitable $\{H_\tau\}_{\tau \in \mathcal{T}}$

Let $\mathcal{T} = GF(2^n)$; $\mathcal{M} = GF(2^n)^s$, i.e.,

- τ is an n-bit string;
- a message consists of s n-bit strings.

Write $M = (M_0, \ldots, M_{s-1})$. Then

$$H_\tau(M) = M_0\tau^{s-1} \oplus M_1\tau^{s-2} \oplus \cdots \oplus M_{s-2}\tau \oplus M_{s-1}.$$

Easy to show that for uniform random τ and $M_1 \neq M_2$,

$$\Pr[H_\tau(M_1) = H_\tau(M_2)] \leq \frac{s-1}{2^n}.$$



How Far Does a Block Cipher Take You?



Is a Block Cipher Sufficient?

Assumption: the block cipher is “perfectly secure” (whatever that may mean).

Is that the end of the story?

No!



Block Cipher and Various Requirements

Block length.

- The block cipher handles n-bit blocks.
- Typically, $n = 128, 192$ or 256 bits.

Message Requirements.

- Handle “long” messages.
- Handle “variable” length messages.
- Handle fixed length messages (a disk sector).



Block Cipher and Various Requirements

Secure Block Cipher.

- The block cipher ensures strong security for n-bit blocks.

Different Security Requirements.

- Privacy only.
- Authentication.
- Authenticated encryption.
- Authenticated encryption with associated data.
- Wide-block encryption.
- Disk sector encryption.
- Format preserving encryption.
- Deterministic authenticated encryption (key wrap problem).
- On-line encryption.
- Other niche requirements.



Modes of Operations

Commonly known modes.

- Electronic codebook mode (ECB).
- Counter mode (Ctr).
- Cipher block chaining mode (CBC).
- Output feedback mode (OFB).
- Cipher feedback mode (CFB).



Things to Note

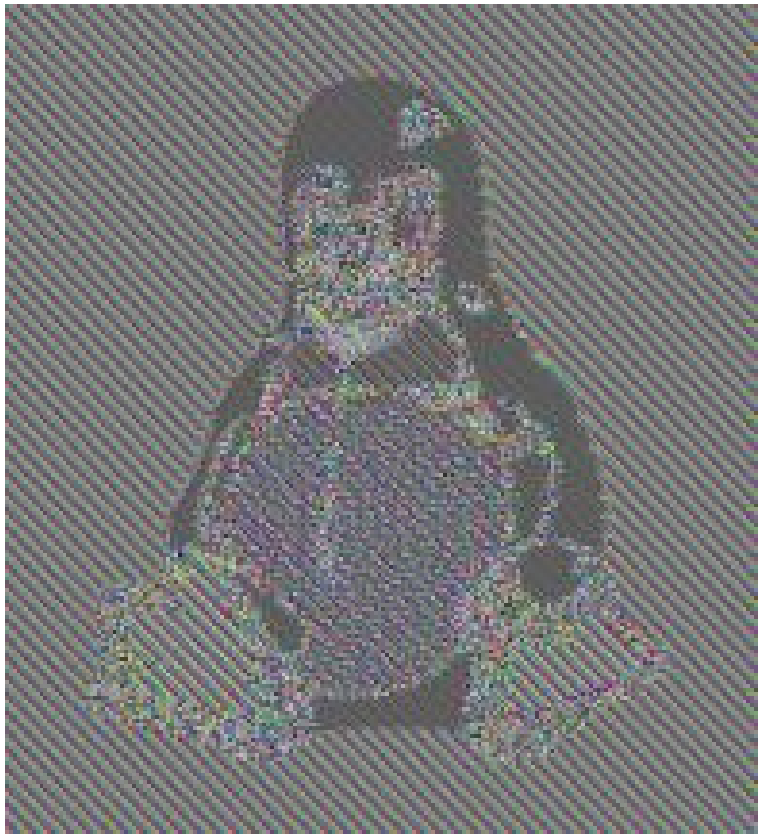
- ECB does not provide privacy.
- Ctr provides privacy but not authentication.
- CBC provides authentication, but, not authenticated encryption.
- Authenticated encryption with associated data?
- Wide block encryption?
- Disk encryption?
- Other security requirements?

There is no single mode which can be used for all applications.



Insecurity of ECB Mode





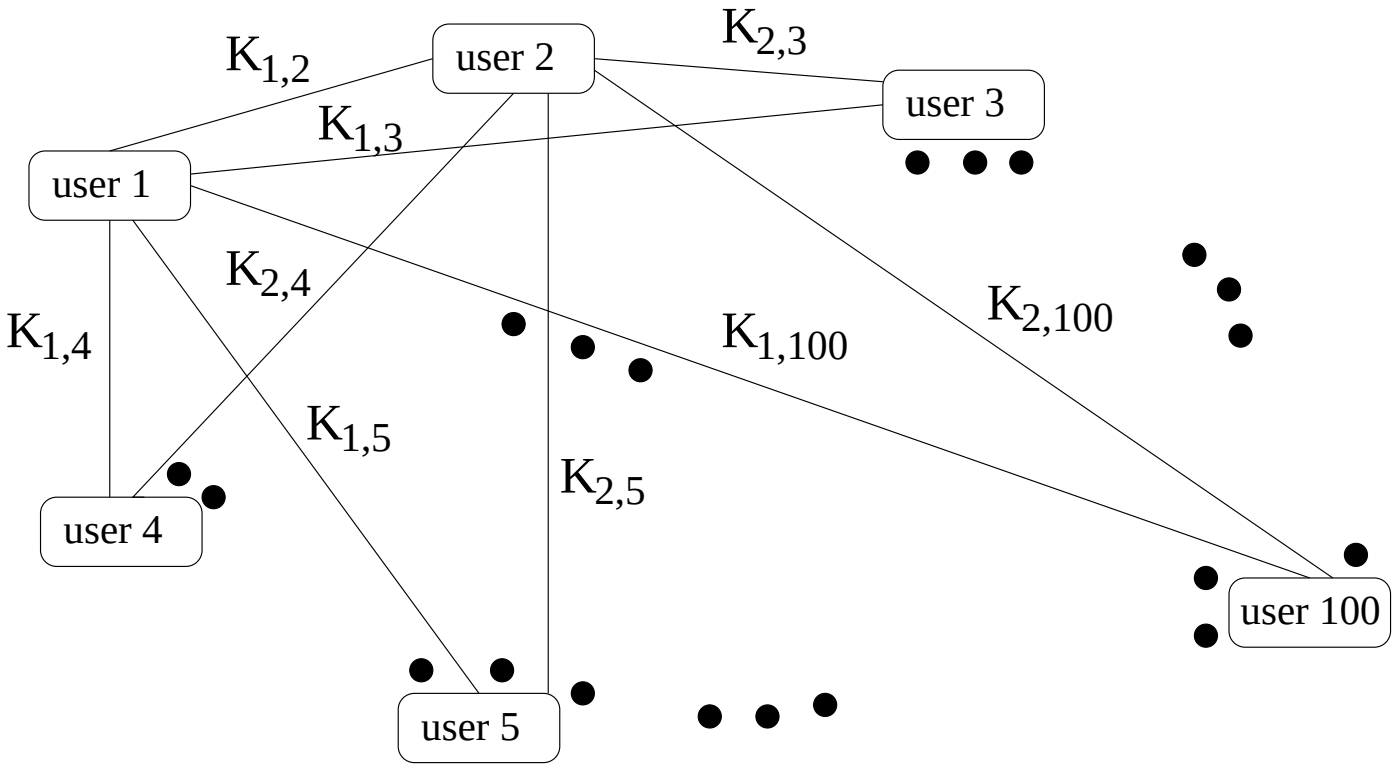
Source: Wikipedia

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation.

Public Key Cryptography: A Paradigm Shift



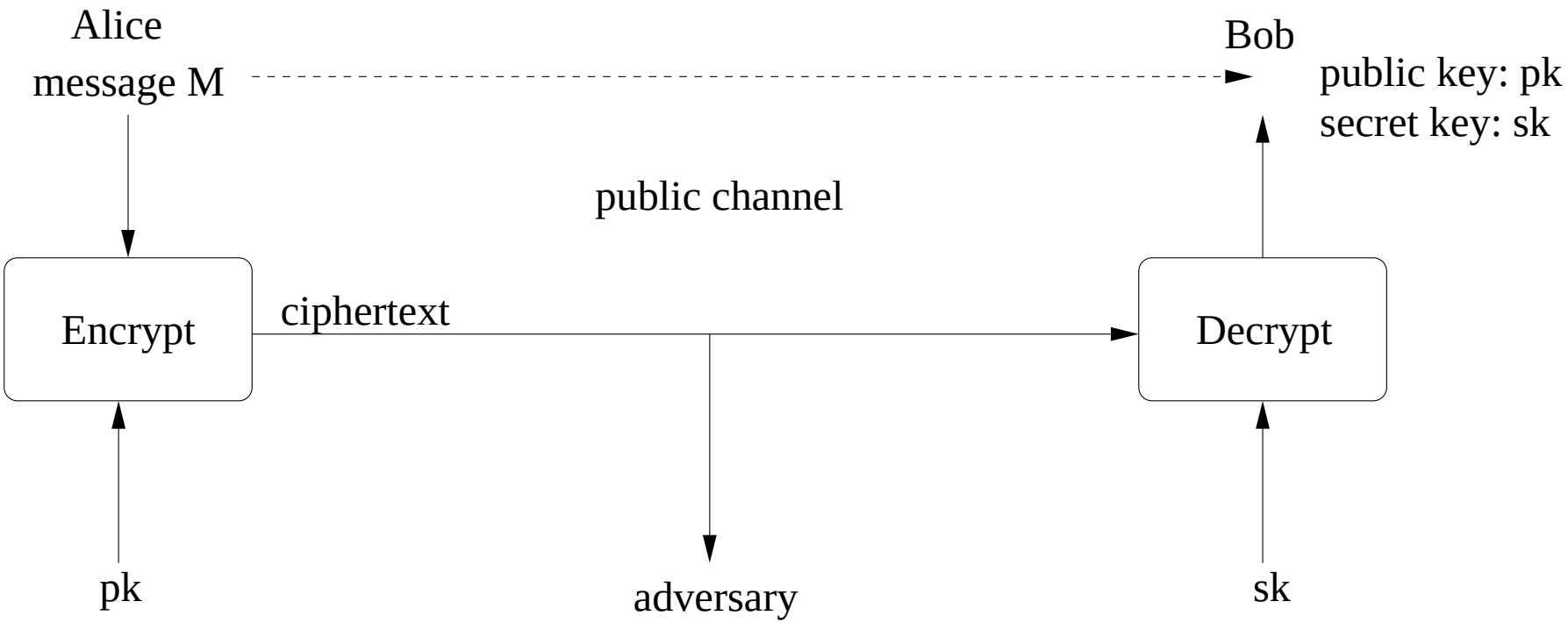
The Key Management Problem



- There are $\binom{100}{2}$ bi-directional links.
- Each link has an associated secret key.
- Each user has to maintain the secrecy of 99 keys.

Change 100 to *n* to see the immensity of the problem!

Public Key Encryption: Overview



Diffie-Hellman Public Key Agreement

Cyclic group $G = \{1, g, g^2, \ldots, g^{p-1}\}$

Alice		Bob
1. Choose secret a;		1. Choose secret b;
2. Compute g^a;		2. Compute g^b;
	send g^a →	
	← send g^b	
3. Compute $K=(g^b)^a=g^{ab}$		3. Compute $K=(g^a)^b=g^{ab}$



ElGamal Public Key Encryption

Alice

Encrypt(M,h).

1. choose random a;
2. set $u = g^a$;
3. set $v = M * h^a$.

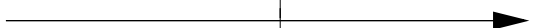
Bob

Set−Up

1. Cyclic group $G = \{1, g, g^2, \ldots, g^{p-1}\}$;
2. Choose secret b;
3. Compute g^b.

   public key: $(g, h=g^b)$; secret key: b.

send (u,v)



Decrypt (u,v).

1. compute $w = u^b = g^{ab} = h^a$;
2. compute $w^{-1} * v = M$.



Computationally Hard Problems

Computational Diffie-Hellman Problem.

Given (g, g^a, g^b) compute g^{ab}.

Decisional Diffie-Hellman Problem. For independent and uniform random a, b, c, distinguish between the distributions:

(g, g^a, g^b, g^{ab}) and (g, g^a, g^b, g^c).

Discrete Logarithm Problem.

Given $(g, h = g^a)$ compute $a \stackrel{\Delta}{=} \log_g h$.



Suitable Groups

- **A suitable subgroup of the multiplicative group of a finite field.**
  - Binary, i.e., $GF(2^n)$ or large characteristics, i.e., $GF(p)$.
  - Sub-exponential algorithm for discrete log problem.

$$\exp\left((\log \#\mathbb{F})^c (\log\log \#\mathbb{F})^{1-c}\right).$$

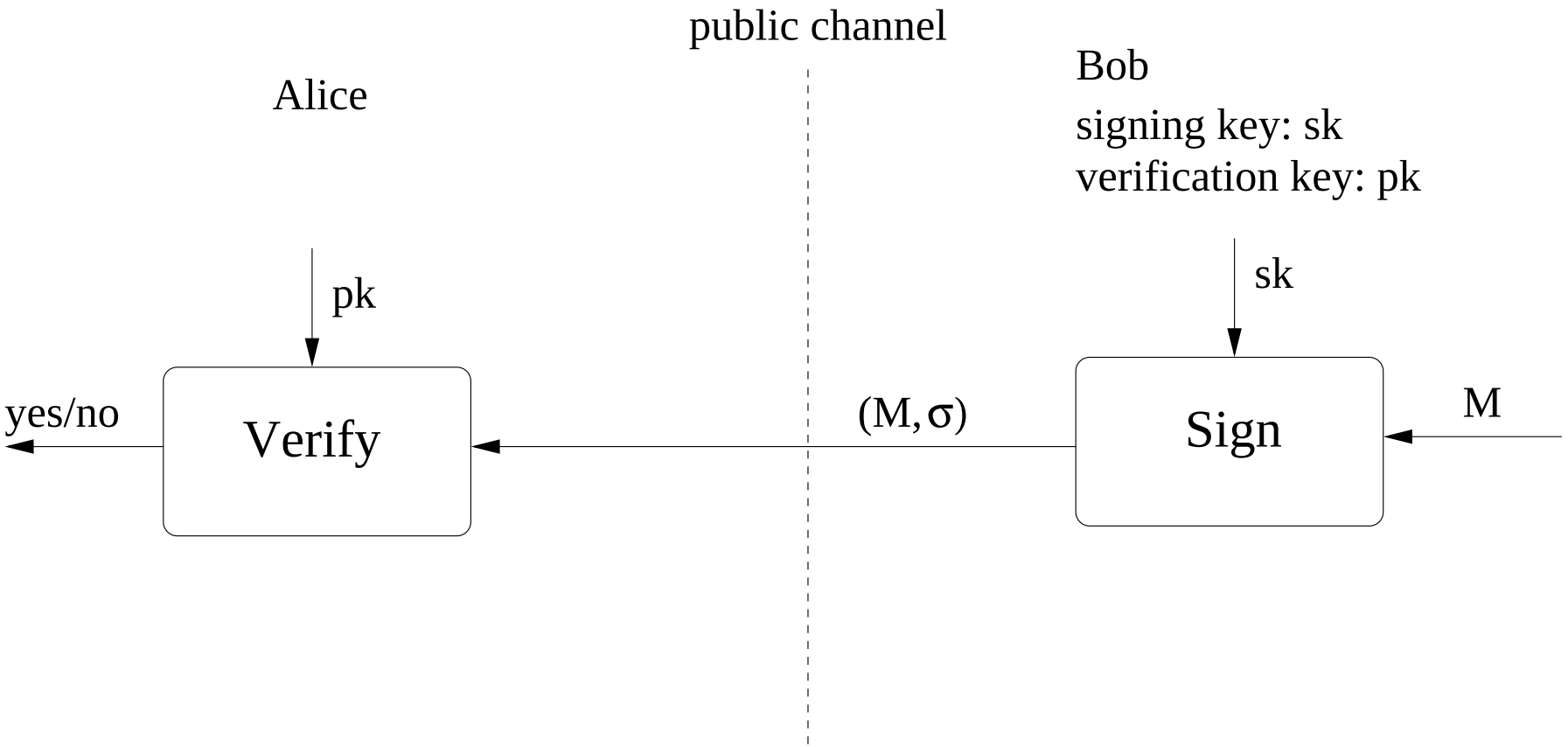
- **Group of points on an elliptic curve over a finite field.**
  $\mathrm{char}(\mathbb{F}) \neq 2, 3$: simplied Weierstraß form:

$$y^2 = x^3 + ax + b \qquad (*)$$

  $a, b \in \mathbb{F}$ and $4a^3 + 27b^2 \neq 0$.
  - Points (x, y) satisfying $(*)$ form a group under a suitably defined addition law.
  - Cryptography is done over a suitable prime order subgroup.
  - No known sub-exponential algorithm for the discrete log problem.
  - Smaller key sizes and faster encryption/decryption algorithms.



Overview of Signature Scheme



ElGamal Signature Scheme

Set-up:

- choose p to be a prime and α to be a generator of $\mathbb{Z}_p^*$;
- let $\beta = \alpha^a$ for some $a \in \{1, \ldots, p-1\}$;
- public key: (p, α, β); secret key: a.

Signing: message x is an integer $1 \leq x \leq p-1$;

- choose secret $k \in \mathbb{Z}_{p-1}^*$.
- signature is (γ, δ) where
  - $\gamma = \alpha^k \bmod p$ and $\delta = (x - a\gamma)k^{-1} \bmod (p-1)$.

Verification: message-signature pair is x and (γ, δ);

- accept if and only if $\beta^\gamma \gamma^\delta \equiv \alpha^x \bmod p$.

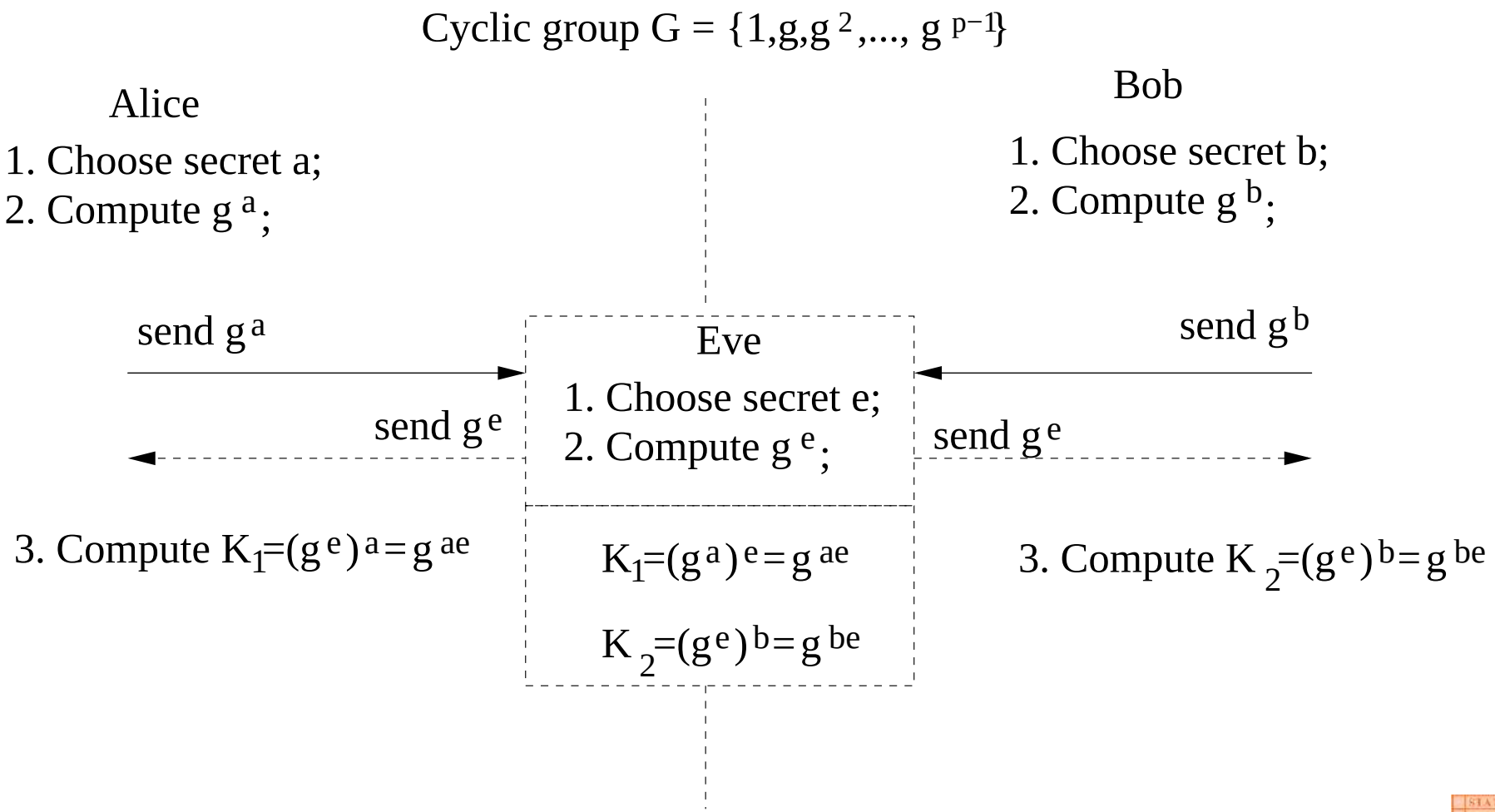
  Verification equation: $\beta^\gamma \gamma^\delta = \alpha^{a\gamma} \alpha^{k\delta} = \alpha^{a\gamma + k\delta} = \alpha^x \bmod p$.



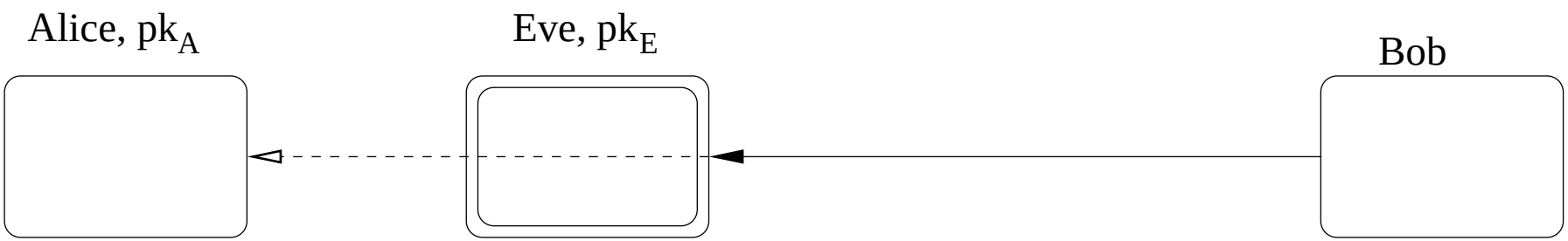
Does PKC Work?



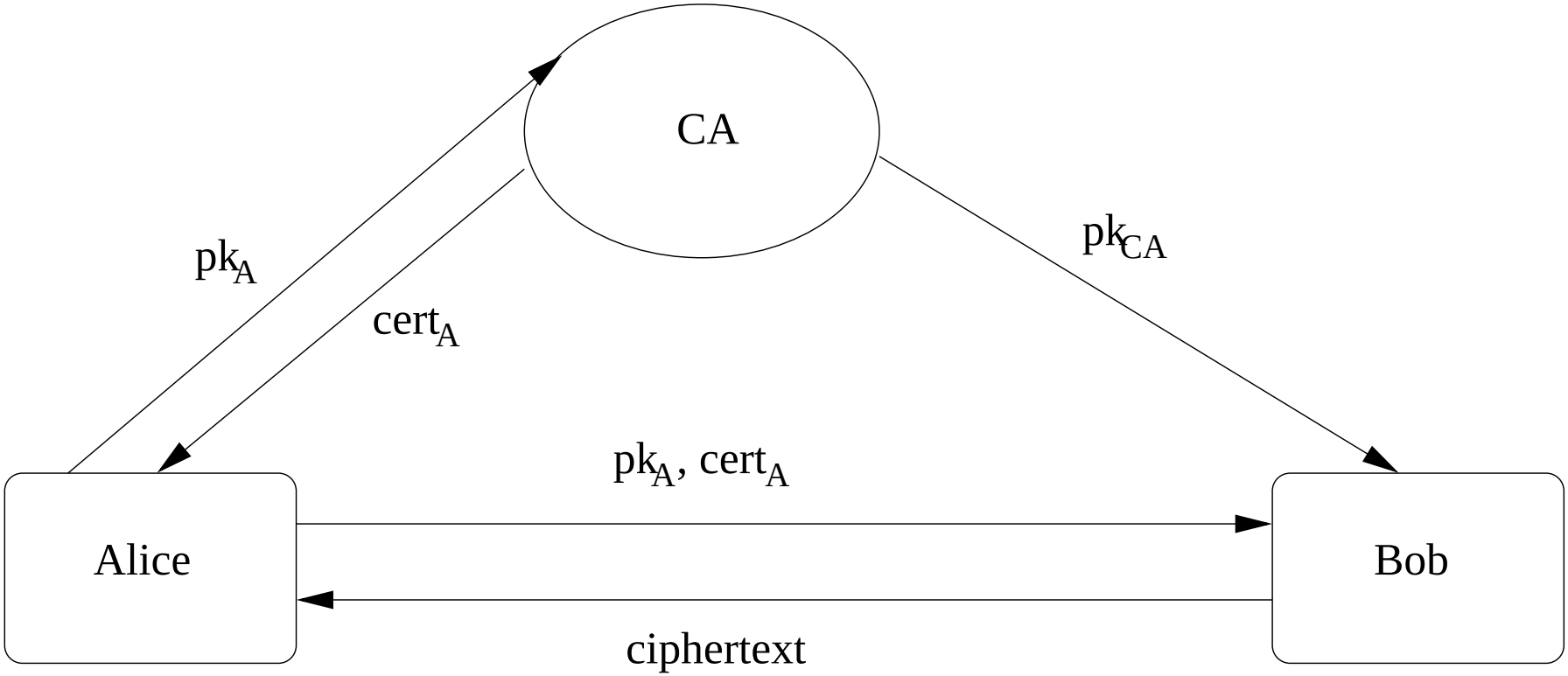
DH-KA: Woman-in-the-Middle



How to Trust a Public Key?



Certifying Authority



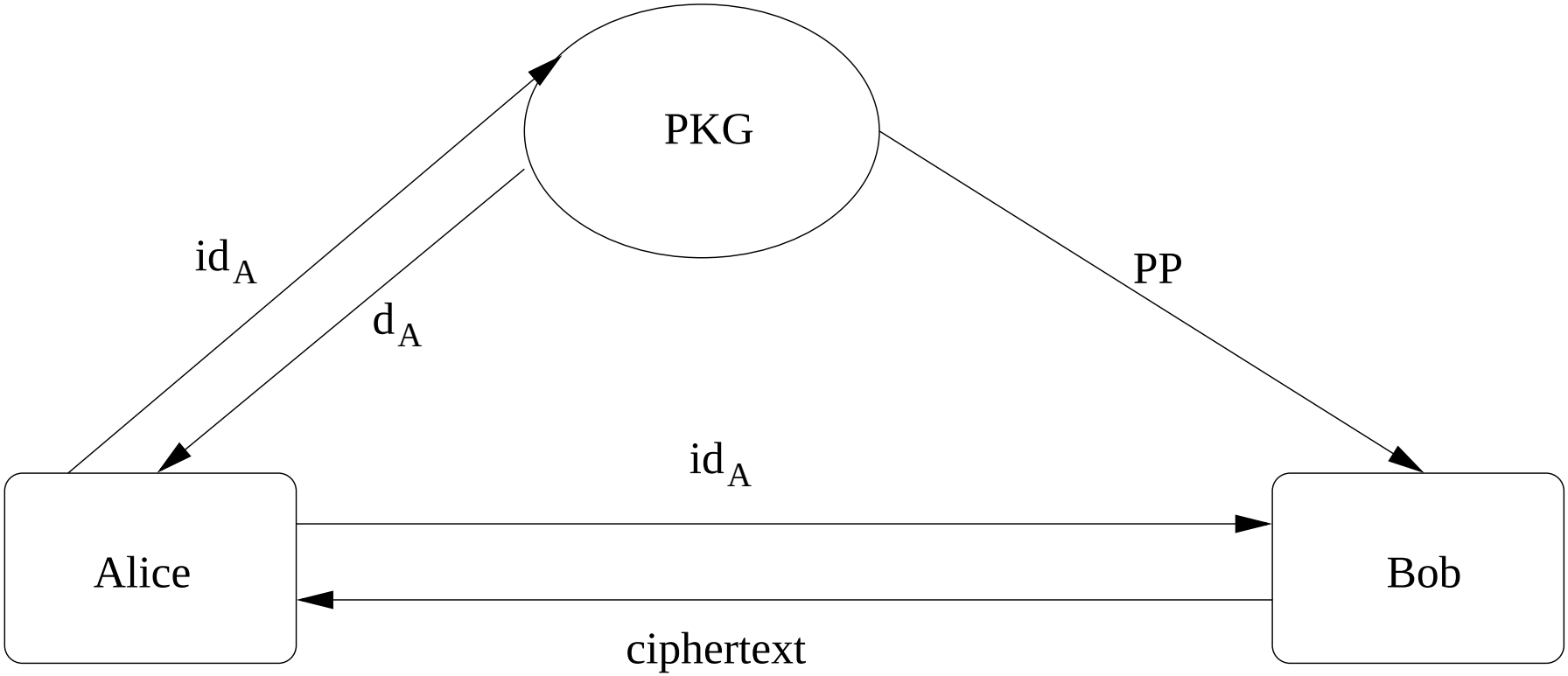
Management of Certificates

- A CA may revoke Alice's certificate.
  - Alice has lost her private key.
  - The validity of the certificate has expired.
  - Other reasons?
- Bob needs to know whether Alice's certificate is "fresh".
  - Certificate revocation list (CRL).
  - Online certificate status protocol (OCSP).
  - One-way hash chains.

Public Key Infrastructure (PKI) covers all of the above.



Identity-Based Encryption



A New Tool



Bilinear Maps

Let G_1, G_2: (additive) cyclic groups; G_T: (multiplicative) cyclic group.

$$e : G_1 \times G_2 \rightarrow G_T$$

- $e(P, Q_1 + Q_2) = e(P, Q_1) \times e(P, Q_2)$.
- $e(P_1 + P_2, Q) = e(P_1, Q) \times e(P_2, Q)$.

If $G_1 = G_2 = G = \langle P \rangle$ and $|G| = p$, then for any $a, b \in \mathbb{Z}_p$

$$e(aP, bP) = e(P, P)^{ab}.$$

- Examples of e arise from Weil and Tate pairings where G_1 and G_2 are groups of points on an elliptic curve and G_T is a subgroup of the multiplicative group of a finite field.



More Computationally Hard Problems

Bilinear Diffie-Hellman Problem.

$$\text{Given } (P, aP, bP, cP) \text{ compute } e(P,P)^{abc}.$$

Decisional Bilinear Diffie-Hellman Problem. For independent and uniform random a, b, c and Z, distinguish between the distributions:

$$(aP, bP, cP, e(P,P)^{abc}) \text{ and } (aP, bP, cP, Z).$$

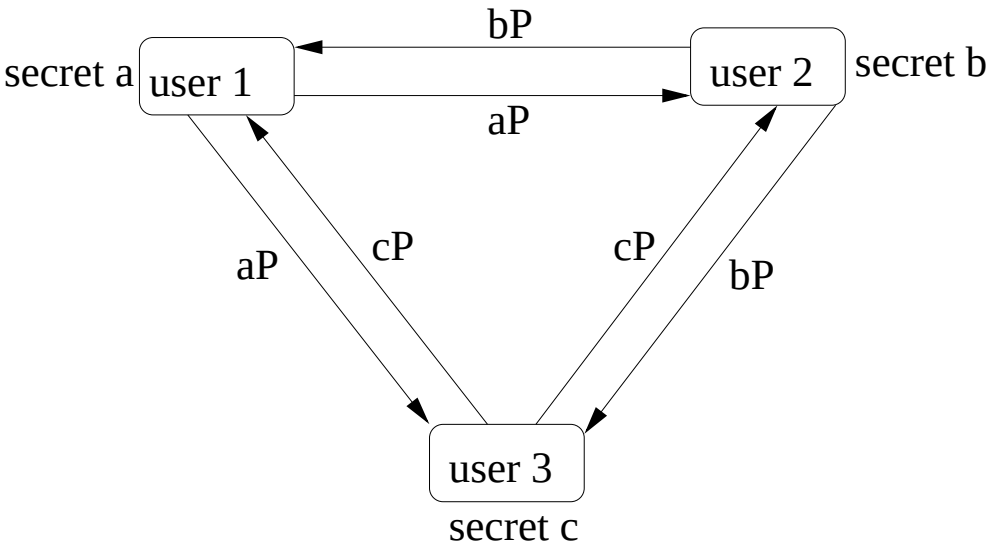
DDH in G is Easy. Given (P, aP, bP, cP), verify

$$e(P, cP) \stackrel{?}{=} e(aP, bP).$$



Joux's 3-Party 1-Round KA

$$G = \langle P \rangle; e : G \times G \rightarrow G_T$$



$$\begin{aligned} e(P,P)^{abc} &= e(bP,cP)^a \text{ (user 1 computes)} \\ &= e(aP,cP)^b \text{ (user 2 computes)} \\ &= e(aP,bP)^c \text{ (user 3 computes).} \end{aligned}$$



Boneh-Franklin IBE

- **Setup:** $\langle P \rangle = G_1$, $s \xleftarrow{\$} \mathbb{Z}_p$, $P_{pub} = sP$
  $$\text{PP} = \langle P, P_{pub}, H_1(), H_2() \rangle, \text{msk} = s.$$

- **Key-Gen:** Given id compute $Q_{id} = H_1(id)$,
  $$d_{id} = sQ_{id}.$$

- **Encrypt:** Choose $r \xleftarrow{\$} \mathbb{Z}_p$,
  $$C = (U = rP, V = M \oplus H_2(e(Q_{id}, P_{pub})^r))$$

- **Decrypt:** Given $C = (U, V)$ and d_{id} compute
  $$V \oplus H_2(e(d_{id}, U)) = M.$$

Pairing Magic.

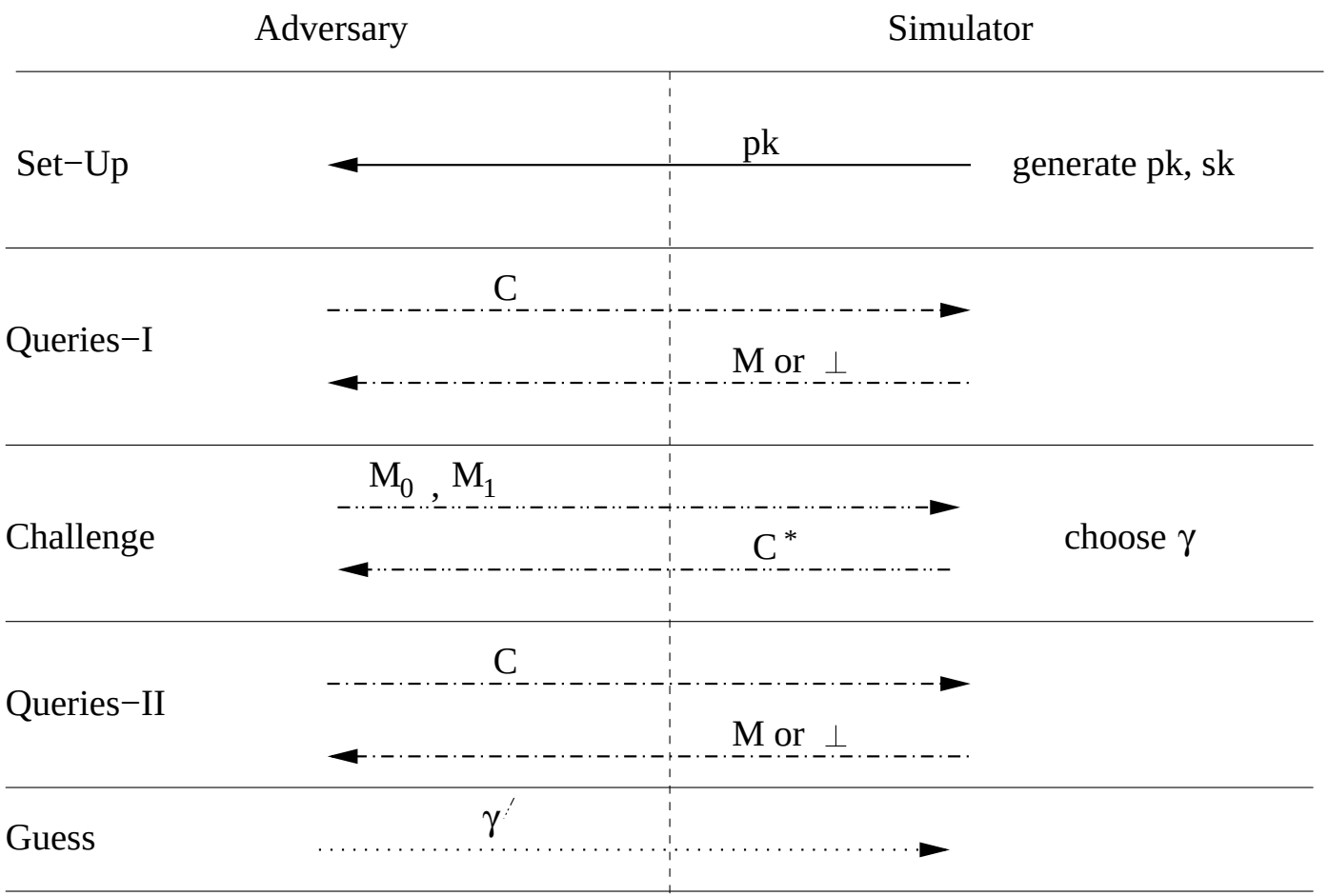
$$e(d_{ID}, U) = e(sQ_{ID}, rP) = e(Q_{ID}, sP)^r = e(Q_{ID}, P_{pub})^r.$$



Some More Formalisms



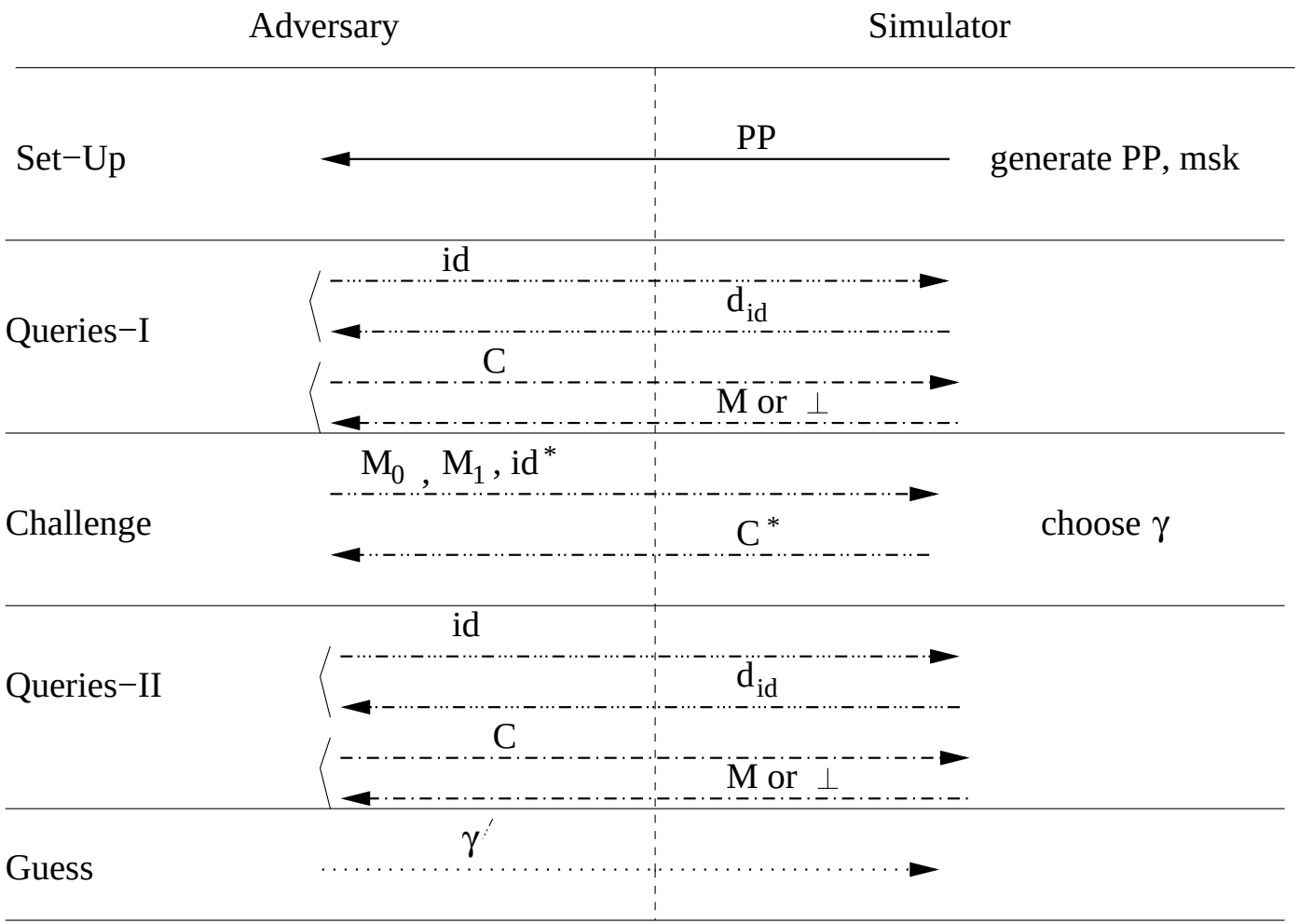
Security Model for PKE



$$\mathsf{Adv}(\mathcal{A}) = \left| \Pr[\gamma = \gamma'] - \frac{1}{2} \right| .$$



Security Model for IBE



$$\mathsf{Adv}(\mathcal{A}) = \left| \Pr[\gamma = \gamma'] - \frac{1}{2} \right| .$$

Security Assurance

If

(smaller protocols are secure
and)
some problem Π is computationally hard

then

the main protocol is secure.

May require additional assumptions.

- Random oracle: assume one (or more) of the functions to be a uniform random function.



Structure of Proofs

$$\frac{\text{A Game Sequence}}{\begin{array}{c} G_0, \\ G_1, \\ \vdots \\ G_k \end{array}}$$

- Let X_i be the event that $\gamma = \gamma'$ in Game G_i. We consider

$$\begin{array}{l} \Pr[X_0], \\ \Pr[X_0] - \Pr[X_1], \\ \vdots \\ \Pr[X_{k-1}] - \Pr[X_k] \\ \Pr[X_k]. \end{array}$$



Structure of Proofs (contd.)

- G_0 is the game which defines the security of the protocol and so

$$\mathsf{Adv}(\mathcal{A}) = |\Pr[\gamma = \gamma'] - 1/2| = |\Pr[X_0] - 1/2|.$$

- G_k is designed such that the bit γ is statistically hidden from the adversary. So,

$$\Pr[X_k] = 1/2.$$

- Games G_{i-1} and G_i differ:
  - the difference is not too much;
  - the adversary should not be able to notice whether he is playing Game G_{i-1} or Game G_i.



Structure of Proofs (contd.)

- More precisely, $\Pr[X_{i-1}] - \Pr[X_i]$ is bounded above by
  - either, the advantage of an adversary in breaking one or the smaller protocols;
  - or, the advantage of solving problem Π.

$$
\begin{aligned}
\mathrm{Adv}(\mathcal{A}) &= |\Pr[X_0] - 1/2| \\
&= |\Pr[X_0] - \Pr[X_k]| \\
&\leq |\Pr[X_0] - \Pr[X_1]| \\
&\quad + |\Pr[X_1] - \Pr[X_2]| \\
&\quad + \cdots \\
&\quad + |\Pr[X_{k-1}] - \Pr[X_k]|.
\end{aligned}
$$



Summary

- A brief history of encryption.
- Briefer mention of authentication.
- Touched upon aspects of algebra and probability.
- Did not mention at all
  - complexity theoretic issues: one-way functions;
  - cryptanalysis of cryptosystems;
  - implementation aspects.
- Hopefully, this summary will be useful.



Thank you for your attention!

