

CIS 5560

Cryptography Lecture 17

Course website:

pratyushmishra.com/classes/cis-5560-s24/

Recap of Last Lecture(s)

- Public Key Encryption
 - Definition of IND-CPA
- ElGamal Encryption
 - Version with message space = $\mathbb{G}$
 - Version with arbitrary message space
- Public Key Encryption from **Trapdoor OWFs**
 - RSA Encryption
 - Arithmetic modulo composites
 - Factoring

Today's Lecture

- Integrity for public key encryption
 - IND-CCA
 - Construction of IND-CCA

Public key encryption

Def: a public-key encryption system is a triple of algs. (G, E, D)

- $\text{Gen}()$: randomized alg. outputs a key pair (pk, sk)
- $\text{Enc}(pk, m)$: randomized alg. that takes $m \in \mathcal{M}$ and outputs $c \in \mathcal{C}$
- $\text{Dec}(sk, c)$: deterministic alg. that takes $c \in \mathcal{C}$ and outputs $m \in \mathcal{M} \cup \{ \perp \}$

Correctness: $\forall (pk, sk)$ output by $\text{Gen}()$, $\forall m \in \mathcal{M}$, $\text{Dec}(sk, \text{Enc}(pk, m)) = m$

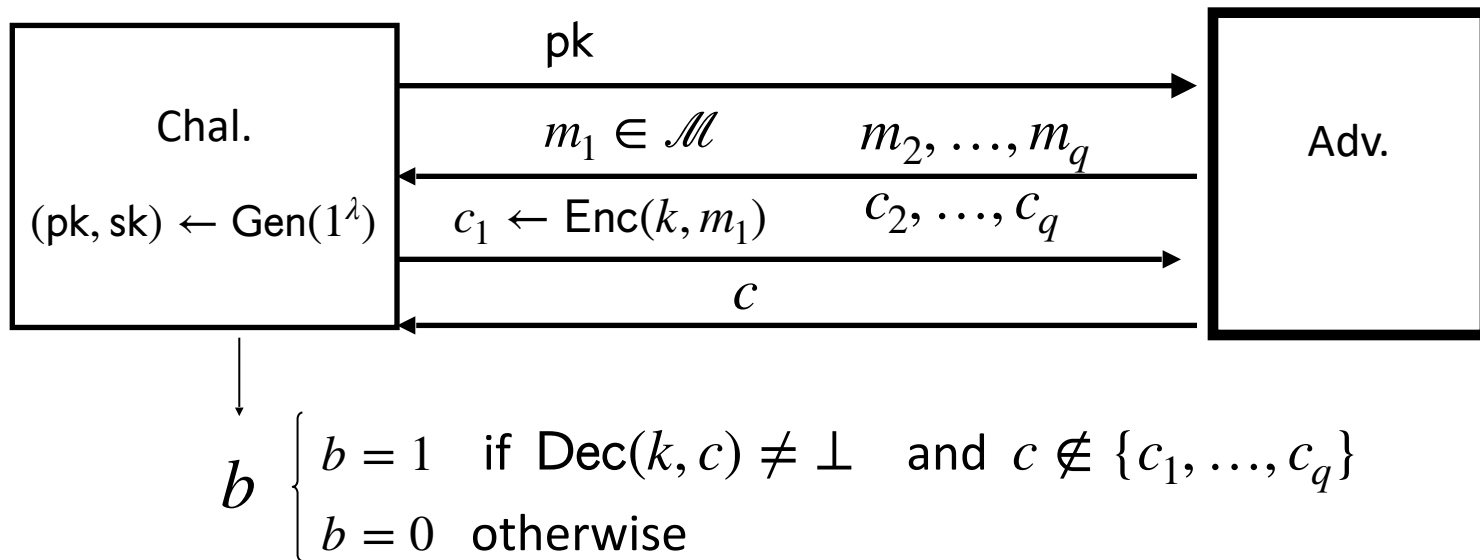
Security: IND-CPA for PKE

For all PPT adversaries $\mathcal{A}$, the following holds:

$$\Pr \left[b = \mathcal{A}(\text{Enc}(\text{pk}, m_b)) \mid \begin{array}{l} (\text{pk}, \text{sk}) \leftarrow \text{Gen}(1^n) \\ \text{Sample } b \leftarrow \{0,1\} \\ (m_0, m_1) \leftarrow \mathcal{A}(\text{pk}) \end{array} \right] \leq \text{negl}(n)$$

What about security against active attacks?

Can we achieve ciphertext integrity?



Def: $(\text{Gen}, \text{Enc}, \text{Dec})$ has **ciphertext integrity** if for all PPT A :

$$\text{Adv}_{\text{CI}}[A] = \Pr[b = 1] = \text{negl}(\lambda)$$

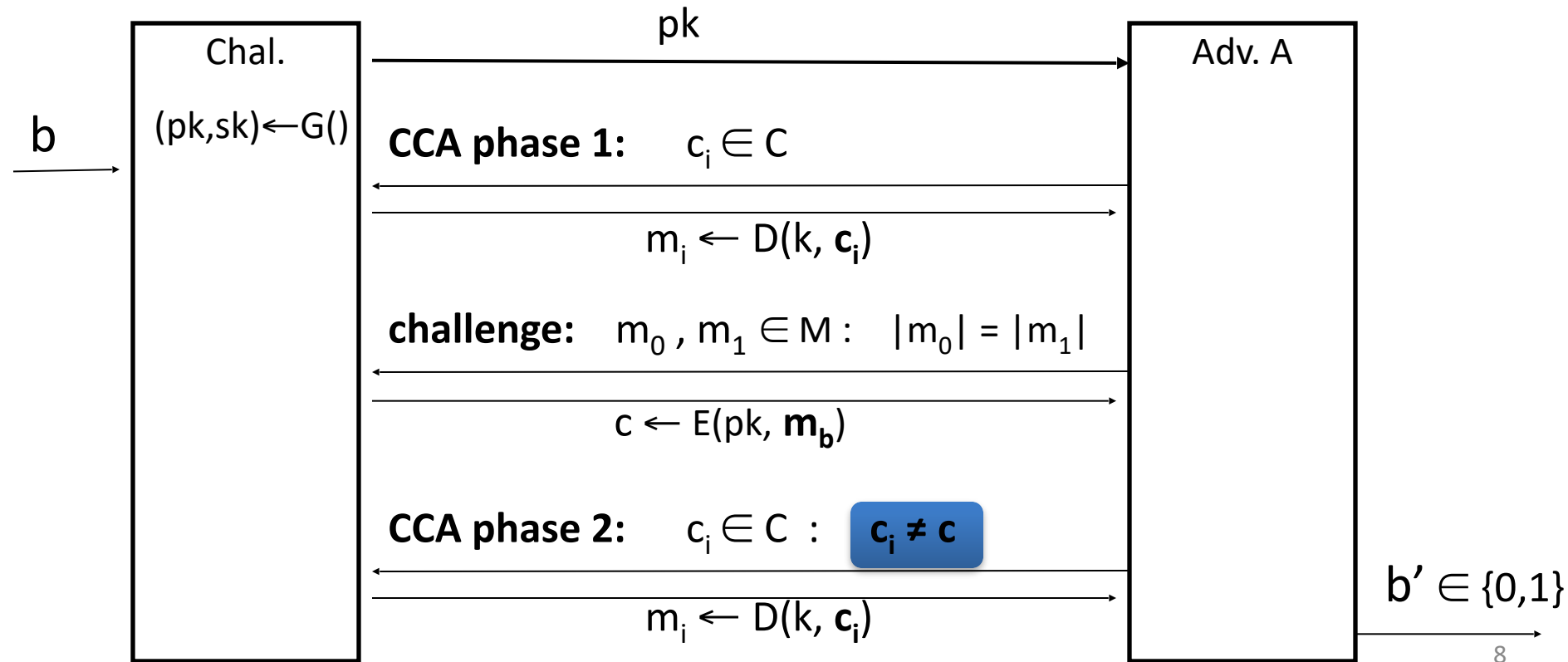
Problem

In public-key settings:

- Attacker **can** *always* create new ciphertexts using pk !!
- So instead: we directly require chosen ciphertext security

PKE Chosen Ciphertext Security: definition

$E = (G, E, D)$ public-key enc. over (M, C)



Construction of IND-CCA secure PKE

The Twin Elgamal system

- $\mathbb{G}$: finite cyclic group of prime order p with generator g
- $(\text{Enc}', \text{Dec}')$: AE scheme with keyspace $\mathcal{K}$
- New ingredient: “Random”-ish hash function $H : \mathbb{G}^2 \rightarrow \mathcal{K}$

Gen(1^n):

1. Sample $a_1, a_2 \leftarrow \mathbb{Z}_p^*$
2. Set $A_1 = g^{a_1}, A_2 = g^{a_2}$
3. Output
(sk = (a_1, a_2) , pk = (A_1, A_2))

Enc(pk, m):

1. Sample $b \leftarrow \mathbb{Z}_p^*$
2. Set $k := H(A_1^b, A_2^b)$
3. Set $c \leftarrow \text{Enc}(k, m)$
4. Output $c' = (g^b, c)$

Dec(sk = (a_1, a_2) , (B, c)):

1. Compute $k = H(B^{a_1}, B^{a_2})$
2. Output $m = \text{Dec}'(k, c)$

Security of Twin ElGamal

Security Theorem:

- If CDH holds in the group $\mathbb{G}$,
 - $(\text{Enc}', \text{Dec}')$ is an AE scheme, and
 - $H : \mathbb{G}^2 \rightarrow \mathcal{K}$ is a “random oracle”
- then twin ElGamal is CCA^{ro} secure.

Cost: one more exponentiation during enc/dec

ElGamal security w/o random oracles?

Can we prove CCA security without random oracles?

- Option 1: use Hash-DH assumption in “bilinear groups”
 - Special elliptic curve with more structure [CHK’04 + BB’04]
- Option 2: use Decision-DH assumption in any group [CS’98]

Further Reading

- The Decision Diffie-Hellman problem. D. Boneh, ANTS 3, 1998
- Universal hash proofs and a paradigm for chosen ciphertext secure public key encryption. R. Cramer and V. Shoup, Eurocrypt 2002
- Chosen-ciphertext security from Identity-Based Encryption. D. Boneh, R. Canetti, S. Halevi, and J. Katz, SICOMP 2007
- The Twin Diffie-Hellman problem and applications. D. Cash, E. Kiltz, V. Shoup, Eurocrypt 2008
- Efficient chosen-ciphertext security via extractable hash proofs. H. Wee, Crypto 2010

Further reading

- A Computational Introduction to Number Theory and Algebra,
V. Shoup, 2008 (V2), Chapter 1-4, 11, 12

Available at [//shoup.net/ntb/ntb-v2.pdf](http://shoup.net/ntb/ntb-v2.pdf)