DI/FCT/UNL
Mestrado Integrado em Engenharia Informática

Confiabilidade de Sistemas Distribuídos / 2º Semestre, 2015/2016
Teste de Avaliação nº 2 (29/Maio/2017)

PARTE I (Sem Consulta, 1 hora)

Questão 1

a) Diga como caracteriza cada uma das seguintes tipologias de cifras homomórficas, enfatizando bem as suas diferenças: (i) *PHE: Partial Homomorphic Encryption; (ii) FHE: Fully Homomorphic Encryption, (iii) SHE: Somewhat Homomorphic Encryption*

PHE:

FHE:

SHE:

b) O sistema criptográfico de Paillier, baseia-se nas mesmas propriedades matemáticas (algébricas) do método de Diffie-Hellman, sobre operações exponenciais modulares (exponenciais modulo M). Gerando-se um par de chaves (pública e privada, de forma semelhante ao processo de geração de números públicos e privados no método de Diffie-Hellman, se usarmos como chave pública o valor do modulo *m* (sendo *m* um número primo) e a base *G* o gerador da raiz primitiva de *m*), então para cifrar a mensagem *x* pode computar-se da seguinte forma:

$E(x) = G^{x} \; r^{m} \mod m^2$, para qualquer valor r = r_i inteiro calculado aleatoriamente tal que r_i pertença ao conjunto de inteiros { 0, ... *m*-1 }

A propriedade homomórfica do método de Paillier pode comprovar-se da seguinte forma (para um dado valor *m)*:

$E(x1)\,E(x2) = (G^{x1} r1^{m} \mod m^2)\,(G^{x2} r2^{m} \mod m^2) = (G^{x1} r1^{m})(G^{x2} r2^{m}) \mod m^2$

$= [\, G^{x1} G^{x2} \, r1^{m} \, r2^{m} \,] \mod m^2 = [\, G^{x1} G^{x2} \mod m^2 \,] \, [r1^{m} \, r2^{m} \,] \mod m^2$

$= [\, G^{(x1+x2)} \mod m^2 \,] \, [\, (r1\, r2)^{m} \mod m^2 \,]$

provando-se então o anterior ser $= [\, G^{(x1+x2 \bmod m)} \; (r1\, r2)^{m}] \mod m$

Logo, escolhendo-se um valor inteiro como produto r1.r2, no mesmo conjunto { 0, ... *m*-1 } teremos que: **E(x1) E(x2) = E (x1 + x2) mod m**

Responda:

b1) Como caracteriza um algoritmo criptográfico que implementasse a construção criptográfica de Paillier, com base na classificação de a) ?

b2) A complexidade computacional identificada é $O(r^n)$ maior do que um cálculo de uma chave pelo método Diffie Hellman ou uma operação de cifra ou decifra com RSA – o que é considerável face a usarmos valores de m da ordem de 1024 ou mesmo 2048 bits, por razões de segurança. Mas por outro lado, o que tem a dizer sobre o espaço de armazenamento requerido para guardar inteiros de 32 bits cifrados que tivessem que ser mantidos no repositório para serem operados cifrados? Justifique.

Questão 2 (Sistema CryptDB)

a) Uma das técnicas utilizadas pelo sistema CryptDB é designada por *Onion-Encryption*. Indique dois objetivos para a utilização dessa técnica de acordo com a argumentação dos autores, e justifique no seu entendimento se esses objetivos são atingidos.

b) Uma das construções de cifras homomórficas parciais usadas pelo sistema CryptDB é designada por DETERMINISTIC ENCRYPTION. Em que consiste essa construção criptográfica ?

Questão 3 (Sistema Byzantium)

a) Diga qual o objetivo principal do sistema Byzantium e quais são as operações básicas suportadas pelo sistema explicando o seu contexto de uso exemplificando com uma possível aplicação que queira tirar partido do sistema.

b) Comparando com o seu conhecimento de quóruns bizantinos (por exemplo sistemas de quóruns com o sistema ABD antes estudado), ao usar uma solução como a do sistema Byzantium, será necessário que os clientes façam operações de leitura em mais do que uma réplica? Porquê?

Questão 4 (Sistema Depsky)

a) Que vantagens tem utilização de um mecanismo do tipo "*secret-sharing*" para conseguir a propriedades de confidencialidade dos objetos fragmentados que estão distribuídos em múltiplas *clouds* de armazenamento? Justifique porque é que o sistema consegue o objetivo tendo por base o modelo de adversário considerado.

b) Comparativamente à utilização de um quórum para replicação de objetos no sistema de armazenamento, que vantagens encontra na utilização de *Erasure Codes*, como mecanismo no modelo do sistema Depsky ? Justifique.

c) Em que consiste a noção de consistência proporcional tal como apresentada como característica do sistema Depsky ? Qual a vantagem ou desvantagem que encontra no sistema suportar essa noção na sua concepção ? Justifique.

PARTE II (Com Consulta, 1 hora)

Questão 5 (Sistema Depsky)

Considere a seguinte afirmação:

"O modelo de base do sistema é do tipo "single-writer/multiple-readers" e para ultrapassar limitações impostas por este modelo de base no caso de aplicações envolvendo múltiplos clientes interagindo com os mesmos objetos armazenados, os autores apresentam uma solução baseada em locks. Porém, devido à noção de consistência proporcional advogada no desenho do sistema, quando o sistema Depsky utiliza por exemplo quatro clouds com heterogeneidade nas garantias de consistência nas operações de escrita/leitura (digamos, uma disponibilizando ***consistência eventual****, outra* ***consistência do tipo read-after-write*** *e as outras com* ***consistência regular****), o mecanismo de locking avançado pelos autores pode não funcionar".*

Concorda ou discorda da afirmação ? Argumente apresentando um exemplo em que a solução não funcionaria e aponte possíveis formas de ultrapassar a dificuldade.

Questão 6 (Sistema Byzantium)

a) Na concepção do sistema a condição de Safety só pode ser garantida se cada transação executar em todas as réplicas no mesmo *snapshot*. Explique Porquê.

b) De acordo com o desenho do sistema, quando se tenta fazer *commit* numa transação numa réplica, como a mesma pode estar a ser executada concorrentemente com outras para as quais a mesma réplica atua como réplica primária, isso pode trazer problemas se a base de dados de suporte utiliza mecanismos de *locking*. Em que medida ou em que circunstâncias tal pode ser um problema ? Justifique.

Questão 7 (CryptDB)

a) Uma das construções de cifras homomórficas parciais usadas pelo sistema CryptDB destina-se a permitir multiplicar inteiros armazenados cifrados. Dada a construção criptográfica em causa, o seu conhecimento da criptografia envolvida e a forma como tem de ser usada, refira-se se incorre em problemas de segurança, mesmo usando chaves de tamanho adequado (exemplo, 2048 bits).

b) No processo de revisão do artigo do CryptDB, quando apresentado ao SOSP 2011, vários revisores apresentaram diversas "limitações" ou "desvantagens". Algumas das questões levantadas encontram-se a seguir (*sic*) como observações de dois dos vários revisores. Para as observações (O1, O2), argumente sobre:

- Se concorda ou discorda da mesma, justificando porquê.
- No que entender concordar como proporia contornar a desvantagem a partir do modelo e arquitetura do sistema, numa aplicação que considerasse o requisito em O1 e a possível aproximação em O2.

O1) *Weakness (sic) "… Indexing operations might not be efficient To support index, the encryption of that column should be OPE. This limits the security. In addition, if there are multi-dimension indexes, the encryption of indexes become complex and makes the insert and delete even more expensive.*

O2) Comment (sic) … *"An interesting question is whether we want to add anonymization of data. I think it could be addressed by CryptDB since it uses onions with multiple forms of encryption with the last layer using a random-based scheme, namely AES. This would break any probability distribution patterns of stored data. If this is the case, then CryptDB not only provides a framework for computation over encrypted data, but also over anonymized data that could be extended. But what if instead of just hiding the columns, the actual data values were encrypted as well before being published? Is it better ?"*