H3 A uppgifter

A-4 Why is the homomorphic property of ElGamal encryption not really suitable in an electronic voting system based on homomorphic encryption?

Svar: Elgamals homomorfiska egenskap är multiplikativ, vilket är en nackdel då röster summeras. ett sätt runt det är att meddelandet är på formen w^{m_1} då blir resultatet av multiplikationen $w^{m_1+m_2}$ tyvärr ställer det till problem då en diskret logaritm måste lösas för att utläsa resultatet vilket är ett beräknings intensivt problem vilket begränsar antalet väljare som kan delta i systemet innan det blir för svårt att ta beräkna resultatet.

A-16 In the slides, two main strategies for making an electronic voting scheme are presented. One is that "the vote is posted on the bulletin board in clear text, but the person casting the vote is anonymous". Describe a scheme like this, and in particular explain why this scheme still ensures "one-voter-one-vote".

Svar: Ett system som implementerar den här typen av röstning är det system som utnyttjar mix nätverk. förfarande är uppdelat i två faser: Registrering och röstning. Väljaren skickar först en publik nyckel PK kryterad med mix kaskadens publika nycklar(k_n): $(R_n, K_n(...(R_3, K_2(R_2, K_1(R_1, PK))))$ För att förhindra att man registrerar sig flera gånger kontrollerar den första mixen identiteten på väljaren. Själva röstnings fasen sker på ett liknande sätt. Fast nu skickar väljaren in Rösten V, PK och signaturen av V med den hemliga nyckeln.

A-18 Why does the blind signature based scheme preserve privacy even if the administrator and the counter cooperate?

Svar: Systemet är uppdelat i två delar: Administrören kontrollerar väljarens identitet och signerar en förblindat värde på formen (x_i, R_i) värdet x_i(commitment) är okänt för administratören. Eftersom det är en blind signatur kan väljaren "extrahera" slumptalet ur signaturen utan att den blir inkorrekt. Räknaren kontrollerar att rösten har lagts av en väljare som godkänts utav administratören genom att kontrollera signaturen till commitmenten Eftersom administratören inte kan veta värdet på commitmenten han signerar kan han inte kollaborera med räknaren för att koppla ihop en väljare med ett värde på x_i. För det krävs kunskap om värdet R_i Vilket endast väljaren har tillgång till.

A-22 In the slides, two main strategies for making an electronic voting scheme are presented. One is that "the vote is posted on the bulletin board in encrypted form, and the person (casting the vote) is not anonymous". Describe a scheme like this, and in particular explain how the vote can be counted without sacrificing privacy/anonymity.

Svar: Lösningen som använder homomorfisk kryptering är av denna typ. Varje väljare krypterar en röst med en homomorfisk kryptering och publicerar sin röst på anslagstavlan tillsammans med sin identifikation. Genom att använda tröskel kryptering kan inte en enskild röst dekrypteras. Endast slutresultatet kan beräknas utav auktoriteterna som betrotts med en del av nyckeln vilket bevarar anonymiteten för väljarna.

A-23 In the homomorphic encryption based scheme, why is it important that voters prove that their vote is correct, e.g., either V_i = -1 or V_i = 1?

Svar: Eftersom att rösten är krypterad och summeringen av röster sker i krypterad form så vore det möjligt att istället kryptera värdet -99999999999999999999999999999999999999999999 om ingen verifikation av V_i ges.

A-24 In the slides regarding homomorphic encryption based voting, it is stated that if the sum of M_i is moderate, we can compute the discrete log. Why does the sum need to be moderate?

Svar: Datorkraften som krävs för att lösa diskreta logaritmer ökar snabbt med större tal vilket gör det orealistiskt att lösa med existerande hårdvara(En av anledningarna problemet med diskreta logaritmer är grundstenen i många asymmetriska krypton).

A-25 Explain why (how) the homomorphic voting scheme in the lecture notes does not have receipt-freeness.

Svar: Eftersom alla röster läggs ut på anslagstavlan kan man lätt kontrollera hur nån har röstat genom att be dem återskapa sin röst med de hemliga värdena m och r.

A-26 Give an example of an electronic voting scheme that provides robustness. Describe how robustness is achieved.

Svar: robusthet är en egenskap som medför att delar av systemet kan fallera eller försöka påverka resultatet utan att det påverkar slutresultat. Systemet som använder homomorfisk kryptering i föreläsnings anteckningarna är en typ av system som är robust. Robustheten stammar ur att systemet använder tröskel kryptering vilket medför att det kan finnas x auktoriteter. för att dekryptera resultatet krävs t stycken auktoriteter. Så länge det finns t auktoriteter som inte fallerat/är korrumperade kan resultatet dekrypteras. Systemet medför också att utomstående kan verifiera att resultatet som publiceras är korrekt.