EE 465: Cryptocurrency and Blockchain Technologies (Autumn 2019)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Endsem Exam : 25 points November 19, 2019

1. (1 point) Suppose Alice owns some bitcoin which are stored in a P2PKH address whose corresponding private key is in a file on her computer. Alice does not want to write down the private key or print it out on a paper, as she is worried someone might steal the paper from her home. She wants to keep the private keys only in electronic form on computers owned only by herself.

   - Alice has three computers where she can store private keys.
   - Alice uses her computers to browse the Internet so there is a chance that a hacker gains access to her computers when she visits a malicious website.
   - Alice's computers may also crash due to a hard disk failure making the files unrecoverable.

   What kind of address should Alice move her bitcoin to such that they are safe as long as **only one of the three** computers gets hacked or crashes? **Specify what information Alice needs to store in each of the three computers.**

   Note: *Alice does not know in advance which computer will get affected. If a computer crashes, Alice loses all information which was stored in that computer. If a computer is hacked, the hacker gains access to all information stored in that computer.*

2. (3 points) Suppose Alice owns some Monero which are stored in two outputs: the first output has one-time address P_1 and Pedersen commitment C_1 and the second output has one-time address P_2 and Pedersen commitment C_2. She wants to send all of the Monero in these outputs (minus transaction fees) to Bob whose long-term address pair is given by (Q_1, Q_2). Describe the procedure used by Alice to construct a transaction containing an MLSAG signature which will send the Monero to Bob. ***Note:*** *The transaction must hide the true source of the funds in a ring of other one-time addresses.*

3. (3 points) Suppose $\mathcal{G}$ is an elliptic curve group with a polynomial-time pairing function $e : \mathcal{G} \times \mathcal{G} \to \mathcal{G}_T$ defined on it where $\mathcal{G}_T$ is a subgroup of a finite field under multiplication. Let the order of $\mathcal{G}$ be a 256-bit prime n and let G be a generator of $\mathcal{G}$.

   Let $P_1, P_2, \ldots, P_N$ be distinct elements of $\mathcal{G}$ such that Alice knows $x \in \mathbb{F}_n$ such that $P_j = xG$ for exactly one $j \in \{1, 2, \ldots, N\}$. Alice creates a linkable ring signature σ over the set of public keys $P_1, P_2, \ldots, P_N$ using x. The linkable ring signature σ contains the key image $I = xH(P_j)$ where $H : \{0,1\}^* \to \mathcal{G}$ is a cryptographic hash function.

   Suppose Bob wants to identify the public key which belongs to Alice in the list $P_1, P_2, \ldots, P_N$, i.e. Bob wants to estimate the index j. Bob does not have ability to compute discrete logarithms of arbitrary elements in $\mathcal{G}$ but he can compute the function e. How can Bob use the pairing function e and the key image I to find j?

4. Suppose N civil contractors are bidding for a contract to build a road for the municipal corporation. The contractor who submits the lowest bid will win the contract. Typically, the contractors are required to submit sealed envelopes containing their bids before a deadline. After the deadline, the envelopes are opened one by one in a meeting attended by all the contractors and the winning bid is declared.

   Consider the following protocol which uses Pedersen commitments instead of sealed paper envelopes.

   (i) Let $\mathcal{G}$ be an elliptic curve group of prime order n which is a 256-bit prime. Assume that the discrete logarithm problem is hard in the group $\mathcal{G}$. Let G and H be generators of the group $\mathcal{G}$ such that the discrete logarithm of H with respect to G is not known.

   (ii) Let $b_i \in \{0, 1, 2, \ldots, 2^{32} - 1\}$ be the bid of the ith contractor for $i = 1, 2, \ldots, N$.

   (iii) Before the deadline, each contractor submits a Pedersen commitment $C_i = x_i G + b_i H$ to the municipal corporation where $x_i \in \mathbb{Z}_n$ is the blinding factor.

   (iv) As soon as each bid is received, the corresponding C_i is displayed on a public notice board in the municipal corporation office.

   (v) After the deadline, each bidder is asked to reveal the blinding factor x_i and bid amount b_i corresponding to its commitment C_i. Failure to reveal these values will disqualify the bidder.

   Answer the following questions.

(a) (2 points) Suppose there are only two bidders, i.e. $N = 2$. Suppose the first bidder's Pedersen commitment C_1 appears on the notice board first and then the second bidder's Pedersen commitment C_2 appears on the notice board. In the meeting after deadline, the first bidder insists that the second bidder should reveal his bid b_2 and blinding factor x_2 first. Why do you think the first bidder says this? How can the second bidder cheat if the first bidder reveals his bid b_1 and blinding factor x_1 first?

Note: *The lower the bid the less the profit a bidder stands to make by taking the road contract. So each bidder wants to bid only slightly less than the other bidder.*

(b) (2 points) Now assume that the number of bidders N is arbitrary. If the blinding factors and amounts are made available to the municipal corporation, how can the corporation convince all the bidders who the winning bidder is without revealing the amounts or blinding factors to them?

(c) (2 points) Suppose the N bidders do not want to reveal their blinding factors or amounts to the municipal corporation. Describe a protocol which can convince everyone of the identity of the winning bidder while revealing only the winning bid amount but not the blinding factors or losing bid amounts. The only information that should be revealed about the losing bid amounts is that they are higher than the winning bid amount.

Hint: *You are allowed to have multiple rounds of communication between the corporation and the bidders.*

5. Two political parties A and B who have formed an alliance want to commit to a power sharing agreement before an election. The power sharing scheme will be described by a pair of integers $a, b \in \{1, 2, \dots, 99\}$ such that $a + b = 100$. These integers represent the percentage of power each party will get if their alliance gets the majority of seats in the election.

Let $\mathcal{G}$ be an elliptic curve group of prime order n which is much larger than 100. Assume that the discrete logarithm problem is hard in the group $\mathcal{G}$. Let G and H be generators of the group $\mathcal{G}$ such that the discrete logarithm of H with respect to G is not known. Party A publishes Pedersen commitment $C_A = x_a G + aH$ for a secret blinding factor $x_a \in \mathbb{Z}_n$. Party B publishes Pedersen commitment $C_B = x_b G + bH$ for a secret blinding factor $x_b \in \mathbb{Z}_n$. The blinding factor of each party is not known to the other (to prevent one party from revealing the other party's share).

(a) ($1\frac{1}{2}$ points) Describe a procedure by which the parties can convince a PPT observer who sees C_A and C_B that the following properties hold, without revealing the blinding factors x_a, x_b or the values a, b to the observer. The procedure should **not reveal** x_a to party B and x_b to party A. Parties A and B **can communicate over a private channel** which is not seen by the observer.

(i) C_A is a Pedersen commitment to a value in the range $\{1, 2, \dots, 99\}$

(ii) C_B is a Pedersen commitment to a value in the range $\{1, 2, \dots, 99\}$

(iii) $C_A + C_B$ is a Pedersen commitment to the value 100.

(b) ($1\frac{1}{2}$ points) Party B wants to send some part of its share b to another party C. Let $c \in \{1, 2, \dots, b-1\}$ be the share of party C which will be committed to by a Pedersen commitment $C_C = x_c G + cH$ for a blinding factor $x_c \in \mathbb{Z}_n$. The remaining share of party B will be committed to by a Pedersen commitment $C'_B = x'_b G + (b - c)H$ for a blinding factor $x'_b \in \mathbb{Z}_n$.

Describe a procedure by which the parties B and C can convince a PPT observer who sees C_B, C'_B, and C_C that the following properties hold, without revealing the blinding factors x_b, x'_b, x_c or the values b, c to the observer. The procedure should **not reveal** x_b, x'_b to party C and x_c to party B. Parties B and C **can communicate over a private channel** which is not seen by the observer.

(i) C_C is a Pedersen commitment to a value in the range $\{1, 2, \dots, 99\}$

(ii) C'_B is a Pedersen commitment to a value in the range $\{1, 2, \dots, 99\}$

(iii) $C'_B + C_C$ is a Pedersen commitment to the same value committed in C_B.

6. (3 points) Let G be a cyclic group of prime order q and generator g, i.e. $G = \langle g \rangle$. For $\alpha, \beta, \gamma \in \mathbb{Z}_q$, we say that $\left(g^\alpha, g^\beta, g^\gamma\right) \in G^3$ is a Diffie-Hellman triple if $\gamma = \alpha\beta$. In other words, a triple $(u, v, w) \in G^3$ is a Diffie-Hellman triple if and only if there exists a $\beta \in \mathbb{Z}_q$ such that $v = g^\beta$ and $w = u^\beta$.

Describe an interactive protocol which is a **honest-verifier zero-knowledge proof of knowledge (HVZKPoK)** for the relation

$$\mathcal{R} = \left\{ ((u, v, w), \beta) \in G^3 \times \mathbb{Z}_q \mid v = g^\beta \text{ and } w = u^\beta \right\}.$$

Note: *You must also prove that the protocol you have described is HVZK and a PoK.*

7. (3 points) Consider the following interactive protocol for proving quadratic non-residuosity of an $x \in \mathbb{Z}_N^*$ where $N = pq$ for odd primes p, q. Let QR_N be the set of quadratic residues modulo N. The verifier does not know the factorization of N.

   - V picks $y \xleftarrow{\$} \mathbb{Z}_N^*$ and a bit $b \xleftarrow{\$} \{0, 1\}$
   - If $b = 0$, V sends $z = y^2$. If $b = 1$, V sends $z = xy^2$
   - For $1 \leq j \leq m$,
     - V picks $r_{j,1}, r_{j,2} \xleftarrow{\$} \mathbb{Z}_N^*$ and computes $\alpha_j = r_{j,1}^2$ and $\beta_j = xr_{j,2}^2$
     - V sends $\text{pair}_j = (\alpha_j, \beta_j)$
   - P sends V a bit string $[i_1, i_2, \ldots, i_m] \in \{0, 1\}^m$
   - V sends P the sequence $v_1, v_2, \ldots, v_m$
     - If $i_j = 0$, then $v_j = (r_{j,1}, r_{j,2})$.
     - If $i_j = 1$, then $v_j = yr_{j,1}$ if $b = 0$. So V sends a square root of $z\alpha_j$
     - If $i_j = 1$, then $v_j = xyr_{j,2}$ if $b = 1$. So V sends a square root of $z\beta_j$
   - P checks the following for each $j \in \{1, 2, \ldots, m\}$
     - If $i_j = 0$, P checks if $(r_{j,1}^2, r_{j,2}^2 x)$ equals pair_j
     - If $i_j = 1$, P checks if $v_j^2 z^{-1}$ is a member of pair_j.
   - If all m checks pass and $z \in QR_N$, P sends $b' = 0$. If $z \notin QR_N$, P sends $b' = 1$
   - V accepts if $b' = b$

   This protocol is **not sound**, i.e. when x is a quadratic residue there exists a cheating prover who can get the verifier to accept with probability 1. So the cheating prover always succeeds in convincing the verifier that a quadratic residue x is a quadratic non-residue. Describe such a cheating prover.

8. (3 points) In the Pinocchio SNARK proof generation, for

   $$v_{mid}(x) = \sum_{k \in \mathcal{I}_{mid}} a_k v_k(x), \quad w_{mid}(x) = \sum_{k \in \mathcal{I}_{mid}} a_k w_k(x), \quad y_{mid}(x) = \sum_{k \in \mathcal{I}_{mid}} a_k y_k(x)$$

   the prover computes $h(x) = \frac{(v_0(x)+v_{io}(x)+v_{mid}(x))\cdot(w_0(x)+w_{io}(x)+w_{mid}(x))-(y_0(x)+y_{io}(x)+y_{mid}(x))}{t(x)}$ and outputs the proof π as

   $$\begin{aligned}\pi &= \left(g^{V_{mid}}, g^{W_{mid}}, g^{Y_{mid}}, g^H, g^{V'_{mid}}, g^{W'_{mid}}, g^{Y'_{mid}}, g^Z \right) \\ &= \left(g_v^{v_{mid}(s)}, g_w^{w_{mid}(s)}, g_y^{y_{mid}(s)}, g^{h(s)}, g_v^{\alpha_v v_{mid}(s)}, g_w^{\alpha_w w_{mid}(s)}, g_y^{\alpha_y y_{mid}(s)}, g_v^{\beta v_{mid}(s)} g_w^{\beta w_{mid}(s)} g_y^{\beta y_{mid}(s)} \right)\end{aligned}$$

   Explain the reason for introducing the scalar γ and group elements $g^\gamma, g^{\beta\gamma}$ in the CRS for checking the following condition in the proof verification procedure

   $$e\left(g^Z, g^\gamma\right) = e\left(g^{V_{mid}} g^{W_{mid}} g^{Y_{mid}}, g^{\beta\gamma}\right)$$

   instead of including group element g^β in the CRS and checking

   $$e\left(g^Z, g\right) = e\left(g^{V_{mid}} g^{W_{mid}} g^{Y_{mid}}, g^\beta\right).$$

   In other words, what will go wrong if we use the second check (after including g^β in the CRS) instead of the first check in the Pinocchio SNARK verification procedure?