Confidential Transactions
Theory Justification

Iftach Haitner*

August 5, 2025

Abstract

[**Iftach's Note: TODO**]

Contents

*Stellar Development Foundation. E-mail: `iftach.haitner@stellar.org`..

1 Introduction

[**Iftach's Note: TODO**]

2 Preliminaries

2.1 Notation

We use calligraphic letters to denote sets, uppercase for random variables, and lowercase for integers and functions. Let $\mathbb{N}$ denote the set of natural numbers. For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$ and $(n) := \{0, \ldots, n\}$. For a relation $\mathcal{R}$, let $\mathcal{L}(\mathcal{R})$ denote its underlying language, i.e., $\mathcal{L}(\mathcal{R}) := \{x \colon \exists w \colon (x, w) \in \mathcal{R}\}$.

2.2 Homomorphic Encryption

An homomorphic encryption is a triplet $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ of efficient algorithms, with the standard correctness and semantic security properties. In addition, there is addition operation denote $+$ over any two (valid) ciphertexts such that for any validly generated public key pk and valid ciphertexts x_0, x_1, it holds that $\mathsf{Enc}_{sk}(x_0) + \mathsf{Enc}_{pk}(x_1) \in \mathrm{Supp}(\mathsf{Enc}_{sk}(x_0 + x_1 \bmod q)$, where $q \in \mathbb{N}$ is efficiently determined by pk.

[**Iftach's Note: Do we really need the homomorphic properties or only for the proofs?**]

3 The Confidential Transaction Protocols

3.1 The Ideal Functionality

Functionality 3.1 ($\mathcal{F}_{\mathsf{ConfTrans}}$: Confidential transactions)**.**

Parties: Issuer I, chain holder C and users $\mathsf{U}_1, \ldots, \mathsf{U}_n$.

Parameters: $p_{\mathsf{num}}, p_{\mathsf{size}} \in \mathbb{N}$.

Init. Upon receiving init from all parties:

1. For each $i \in [n]$: $\mathsf{avlBlance}_i, \mathsf{pndBalance}_i \leftarrow 0$, $\mathsf{transnum}_i \leftarrow 0$, and $\mathsf{log}_i \leftarrow \emptyset$.
2. $\mathsf{log} \leftarrow \emptyset$.

Issue. Upon receiving $(\mathsf{sid}, \mathsf{issue}, x, d)$ from C and I:

1. Assert($x \in (p_{\mathsf{num}})$, $\mathsf{transnum} \leq p_{\mathsf{size}}$ and $d \in [n]$).
2. $\mathsf{transnum}^{++}$.
3. $\mathsf{pndBalance}_d \mathrel{+}= x$.
4. Set $\mathsf{log} \cup= (\mathsf{sid}, \mathsf{issue}, x, d)$.

Transfer. Upon receiving $(\mathsf{sid}, \mathsf{transfer}, d)$ from C and U_s, with U_s using private input x.

1. Assert($x \in (p_{\mathsf{num}})$, $\mathsf{transnum} \leq p_{\mathsf{size}}$, $\mathsf{avlBlance}_s \geq x$ and $d \in [n]$).
2. $\mathsf{transnum}^{++}$.
3. $\mathsf{avlBlance}_s \mathrel{-}= x$.
4. $\mathsf{pndBalance}_d \cup= x$.
5. Set $\mathsf{log}_d \cup= (\mathsf{sid}, \mathsf{transfer}, s, x)$
6. Set $\mathsf{log} \cup= (\mathsf{sid}, \mathsf{transfer}, s, d)$

Rollover. Upon receiving $(\mathsf{sid}, \mathsf{rollover})$ from party U_i and C, party C

1. $\mathsf{transnum} \leftarrow 0$.
2. Set $\mathsf{avlBlance}_i \mathrel{+}= \mathsf{pndBalance}_i$.
3. Set $\mathsf{pndBalance}_i \leftarrow 0$.
4. Set $\mathsf{log} \cup= (\mathsf{sid}, \mathsf{rollover}, i)$

Withraw. Upon receiving $(\mathsf{sid}, \mathsf{withraw}, x)$ from party U_i and C, party C

1. Assert($x \in \mathbb{N}$, $\mathsf{avlBlance}_i \geq x$ and $i \in [n]$).
2. $\mathsf{avlBlance}_i \mathrel{-}= x$.
3. Set $\mathsf{log} \cup= (\mathsf{sid}, \mathsf{withraw}, i, x)$

History. Upon receiving $(\mathsf{sid}, \mathsf{history})$ from party P_i and C:

Send $(\mathsf{log}, \mathsf{log}_i)$ to P_i.

Audit. [**Iftach's Note: Later**]

3.2 The Protocol

Throughout, we fix a security parameter κ and omit is from the notation. We also fix an homomorphic encryption scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ over $\mathbb{Z}_q$ with randomness domain $\mathcal{D}$. We require that $\mathsf{Dec}_{sk}(\overline{A})$ outputs $(a; r)$ such that $\overline{A} = \mathsf{Enc}(a; r)$.

Protocol 3.2 ($\Pi_{\mathsf{ConfTrans}}$: Confidential transactions)**.**

Parties: Issuer I, chain-holder C and users $\mathsf{U}_1, \ldots, \mathsf{U}_n$.

Subprotocols: See below.

Init. We use POK for the relation:

Key generation: $\mathcal{R}_{\mathsf{KeyGen}} = \{(pk, w)) \colon \mathsf{KeyGen}(w) = (\cdot, pk)\}$.

Protocol 3.3 ($\Pi_{\mathsf{ConfTrans}}$.Init)**.**

Participating parties. All parties.

Proofs: $\Pi^{\mathsf{ZK\text{-}POK}}_{\mathcal{R}_{\mathsf{KeyGen}}}$.

Algorithms: KeyGen.

Operation:

1. P_i, for all $i \in [n]$:
   (a) Set $(pk_i, sk_i) \xleftarrow{\text{R}} \mathsf{KeyGen}(r_i)$ for $r_i \xleftarrow{\text{R}} \mathcal{D}$.
   (b) Store sk_i.
   (c) Let $\pi_i \xleftarrow{\text{R}} \mathsf{P}^{\mathsf{ZK\text{-}POK}}_{\mathcal{R}_{\mathsf{KeyGen}}}(pk_i, r_i)$.
   (d) Send (pk_i, π_i) to C.
2. C:
   (a) Call $\{\mathsf{V}^{\mathsf{ZK\text{-}POK}}_{\mathcal{R}_{\mathsf{KeyGen}}}(pk_i, \pi_i)\}_{i\in[n]}$. Abort and publish i, if the i^{th} proof is not verified.
   (b) Store $\{pk_i\}_{i\in[n]}$.
3. C:
   (a) Broadcast $\{\overline{P}_i \leftarrow 0, \overline{P}_i \xleftarrow{\text{R}} \mathsf{Enc}_{pk_i}(0), \overline{B}_i \leftarrow \emptyset\}_{i\in[n]}$.
   (b) Broadcast $\mathsf{log} \leftarrow \emptyset$.

Issue.

Protocol 3.4 ($\Pi_{\mathsf{ConfTrans}}$.Issue)**.**

Participating parties. I and C.

C's input. sid, $x \in \mathbb{N}$ and $i \in [n]$.

Operation:

1. I: Send (x, i) to C.
2. C:
   (a) Assert($x \in [p_{\mathsf{size}}]$ and $\overline{P}_i \leq p_{\mathsf{size}}$)
   (b) Set $\overline{P}_i \mathrel{+}= \mathsf{Enc}_{pk_i}(x)$).
   (c) Publish $\mathsf{log} \cup= (\mathsf{sid}, \mathsf{issue}, x, i, \overline{P}_i)$.

Transfer. We use proof and POK for the following relations:

In range. $\mathcal{R}_{\mathsf{rp}} = \{((pk, A), (a, r)) \colon \mathsf{Enc}_{pk}(a; r) = A \wedge a \in [p_{\mathsf{size}}]\}$, i.e., encryption of values in $[p_{\mathsf{size}}]$.

Equality. $\mathcal{R}_{\mathsf{eq}} = \left\{((pk^0, pk^1, A^0, A^1), (a, r^0, r^1)) \colon \forall i \in \{0, 1\}\ \mathsf{Enc}_{pk^i}(a; r^i) = A^i\right\}$, i.e., encryptions of the same pair under different public keys.

Larger than. $\mathcal{R}_{\mathsf{lrger}} = \{((pk, A^0, A^1), (a^0, r^0, a^1, r^1)) \colon \forall i \in \{0,1\}\ \mathsf{Enc}_{pk}(a^i; r^i) = A^i \wedge a^1 - a^0 \in [q]\}$, i.e., encryptions of the pair of values (a_0, a_1), under the same public key, with $a_1 \geq a_0$.

Protocol 3.5 ($\Pi_{\mathsf{ConfTrans}}$.Transfer)**.**

Participating parties: P_s and C.

Proofs: $\Pi^{\mathsf{ZK}}_{\mathcal{R}_{\mathsf{rp}}}$,$\mathsf{P}^{\mathsf{ZK}}_{\mathcal{R}_{\mathsf{eq}}}$,$\mathsf{P}^{\mathsf{ZK}}_{\mathcal{R}_{\mathsf{lrger}}}$

Algorithms: Dec.

Common input: $d \in [n]$.

P_s's private input. $x \in \mathbb{N}$.

Operation:

1. P_s:
   (a) $X_d \xleftarrow{\text{R}} \mathsf{Enc}_{pk_d}(x; r)$ for $r^d \xleftarrow{\text{R}} \mathcal{D}$.
   (b) $\pi^{\mathsf{rp}} \xleftarrow{\text{R}} \mathsf{P}^{\mathsf{ZK}}_{\mathcal{R}_{\mathsf{rp}}}((pk_d, X_s, p_{\mathsf{size}}), (x, r))$.
   (c) $X_s \xleftarrow{\text{R}} \mathsf{Enc}_{pk_s}(x; r)$ for $r^s \xleftarrow{\text{R}} \mathcal{D}$.
   (d) $\pi^{\mathsf{eq}} \xleftarrow{\text{R}} \mathsf{P}^{\mathsf{ZK}}_{\mathcal{R}_{\mathsf{eq}}}((pk_s, pk_d, X_s, X_s), (x, r_s, r_d))$.
   (e) $(b, r^b) \leftarrow \mathsf{Dec}_{sk_s}(\overline{B}_s)$.
   (f) $\pi^{\mathsf{lrger}} \xleftarrow{\text{R}} \mathsf{P}^{\mathsf{ZK}}_{\mathcal{R}_{\mathsf{lrger}}}((pk_s, X_s, \overline{B}_s), (x, r_s, r_b))$.
   (g) Send $(X_s, X_d, \pi^{\mathsf{rp}}, \pi^{\mathsf{eq}}, \pi^{\mathsf{lrger}})$ to C.
2. C:
   (a) Call $\mathsf{V}^{\mathsf{ZK\text{-}POK}}_{\mathcal{R}_{\mathsf{rp}}}((pk_d, X_s, p_{\mathsf{size}}), \pi^{\mathsf{rp}})$,
   $\mathsf{V}^{\mathsf{ZK\text{-}POK}}_{\mathsf{eq}}((pk_s, pk_d, X_s, X_s), \pi^{\mathsf{rp}})$ and $\mathsf{V}^{\mathsf{ZK\text{-}POK}}_{\mathcal{R}_{\mathsf{lrger}}}((pk_s, X_s, \overline{B}_s), \pi^{\mathsf{rp}})$.
   (b) Set $U_s \mathrel{-}= X_s$.
   (c) Set $\overline{P}_d \mathrel{+}= X_d$.
   (d) Publish $\mathsf{log} \cup= (\mathsf{sid}, \mathsf{transfer}, s, d, U_s, \overline{P}_d)$.

Rollover.

Protocol 3.6 ($\Pi_{\mathsf{ConfTrans}}$.Rollover)**.**

Participating parties. P_i and C.

Operation:
C:

1. $\overline{B}_i \mathrel{+}=$
   oP_i.

2. $\overline{P}_i \mathrel{-}= \overline{P}_i$.

3. $\mathsf{log} \mathrel{+}= (\mathsf{sid}, \mathsf{rollover}, i, \overline{B}_i, \overline{P}_i)$

History.

Protocol 3.7 ($\Pi_{\mathsf{ConfTrans}}$.History)**.**

Participating parties. P_i and C.

Operation: C: send log to P_i.

Audit. [**Iftach's Note: TODO**]

3.2.1 Security of Protocol 3.2

Theorem 3.8 (Security of Protocol 3.2)**.** [**Iftach's Note: TODO**]

4 The ElGammal-Based Additive Homomorphic Encryption

In this section we define the (efficient) additive homomorphic encryption scheme based on ElGammal multiplicative homomorphic encryption scheme. [**Iftach's Note: give citations**]

The idea is to bootstrap the so-called *ElGammal in-the exponent* additive homomorphic encryption scheme,[1] which in turn is based on the ElGammal multiplicative homomorphic encryption scheme, that lacks efficient decryption algorithm, by splitting the plain text into small "chunks". That is, we present message $m \in Z_t$ as
$\sum_{i\in(t/c)} 2^{ic} \cdot m_i$, where c, the chunk size, is some integer that divides $[t]$, and encrypt using additive homomorphic EG each of the m_i. To decry $\overline{M} = (M_0, \ldots, M_{t/c})$, one

1. Decrypt each M_i to get $m_i \cdot G$.

2. Use brute force to find m.[2]

3. Reconstruct m.

4.1 ElGammal In-the-Exponent Scheme

Throughout we fix a cyclic additive q-size group $\mathcal{G}$ with generator G. The ElGammal in-the-exponent scheme $(\mathsf{EgGen}, \mathsf{EgEnc}, \mathsf{EgDec})$ is define as follows:

Key generation: $\mathsf{EgGen}()$ samples $e \overset{\text{R}}{\leftarrow} \mathbb{Z}_q$, and outputs $(e, e \cdot G)$.

Encriyption: $\mathsf{EgEnc}_E(m)$ samples $e \overset{\text{R}}{\leftarrow} \mathbb{Z}_q$, and outputs $\widetilde{M} \leftarrow (r \cdot G, r \cdot E + m \cdot G)$

[1] It is called ElGamal "in-the-exponent" due to typical multiplicative group notation. Here use additive group notation, but keep the name for historical reason.

[2] One can use standard processing to speed-up this part from c group operations to $\sqrt{c}$ operations, or even [**Iftach's Note: cite**] to $\sqrt[3]{c}$.

Decription: $\mathsf{EgDec}_e(\widetilde{M})$,

1. Let $M \leftarrow \widetilde{M}_2 - e \cdot \widetilde{M}_2$.
2. Find (using brute force) m so that $m \cdot G = M$.
3. Output m.

4.2 The Scheme

In the following we fix $t, c \in \mathbb{N}$ with $t \leq q$ and $\ell \leftarrow t/c \in \mathbb{N}$. The encryption scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is defined as follows:

Key generation: $\mathsf{KeyGen}()$: act as $\mathsf{EgGen}()$.

Encryiption: $\mathsf{Enc}_{\mathsf{pk}}(m)$

1. Compute $m_0, \ldots, m_{\ell-1}$ do that $m = \sum_{i \in (\ell)} 2^{ic} \cdot m_i$.
2. For each $i \in (\ell)$: let $\widetilde{M}_i \overset{\mathrm{R}}{\leftarrow} \mathsf{EgEnc}_{\mathsf{pk}}(m_i)$.
3. Output $\overline{M} \leftarrow (\widetilde{M}_0, \ldots, \widetilde{M}_{\ell-1})$.

Decription: $\mathsf{EgDec}_{\mathsf{sk}}(\overline{M})$

1. For each $i \in (\ell)$: let $m_i \overset{\mathrm{R}}{\leftarrow} \mathsf{EgDec}_{\mathsf{sk}}(\overline{M}_i)$.
2. Let $m \leftarrow \sum_{i \in (\ell)} 2^{ic} \cdot m_i$.
3. Output m.

4.3 Proofs

Knowledge of secret key.

Task: ZKPOK for $\mathcal{R}_{\mathsf{KeyGen}} = \{(pk, w)) \colon \mathsf{KeyGen}(w) = (\cdot, pk)\}$.

Proof: Apply the (standard) ElGammal POK for the secret key relation.

Knowledge of plain text.

Task: ZKPOK for $\mathcal{R}_{\mathsf{enc}} = \big\{((pk, A), (a, r)) \colon \mathsf{Enc}_(pk)(a; r) = A\big\}$.

Proof: On plaintext $\overline{A}$, for each $\overline{A}_i$ apply the standard EG POK for the ciphertexts relation.

Decryptability.

Task: ZKP for $\mathcal{R}_{\mathsf{dec}} = \big\{((\mathsf{pk}, \overline{A}), (\overline{a}, \overline{w})) \colon \forall i \in (\ell) \mathsf{EgEnc}_{\mathsf{pk}}(\overline{a}_i; \overline{r}_i) = \overline{A}_i \wedge \overline{w}_i \in (2^c)\big\}$.

Proof: On plaintext $\overline{A}$, for each $\overline{A}_i$: apply EG range proof to show that th encrypted plaintext is in (2^c).

Equality.

Task: ZKP for $\mathcal{R}_{\mathsf{eq}} = \big\{((pk^0, pk^1, A^0, A^1), (a, r^0, r^1)) \colon \forall i \in \{0,1\}\ \mathsf{Enc}_{pk^i}(a; r^i) = A^i\big\}$.

Proof: On input $(\mathsf{pk}^0, \mathsf{pk}^1, \overline{A}^0, \overline{A}^1, a, \overline{r}_0, \overline{r}_1)$

1. For both $j \in \{0,1\}$:
   (a) Let $a \leftarrow \sum_i 2^c \cdot a_i$

Task: ZK for $\mathcal{R}_{\mathsf{rp}} = \{((pk, A), (a, r)) \colon \mathsf{Enc}_{pk}(a; r) = A \wedge a \in [p_{\mathsf{size}}]\}$.

Proof: On public key sk, for each $i \in [\ell]$ apply the (standard) ElGammal ZKP for the secret key relation.

Larger than.

Task: POK for $\mathcal{R}_{\mathsf{lrger}} = \big\{((pk, A^0, A^1), (a^0, r^0, a^1, r^1)) \colon \forall i \in \{0,1\}\ \mathsf{Enc}_{pk}(a^i; r^i) = A^i \wedge a^1 - a^0 \in [q]\big\}$.

Proof:

4.4 Adjusting Section 3.2