Lelantus Spark Audit

Mikerah Quintyne-Collins, Karl Yu, Er-Cheng Tang

HashCloak Inc

Desember 2021

1 Pendahuluan

Lelantus Spark adalah protokol privasi generasi berikutnya dari Firo blockchain yang bertujuan untuk meningkatkan privasi penggunanya dengan fitur-fitur tambahan. Beberapa fitur baru dari protokol Lelantus Spark adalah skema multisignature, dan fungsionalitas pengungkapan yang selektif. HashCloak telah dilibatkan oleh tim Firo untuk melakukan audit terhadap kriptografi Lelantus Spark. Kami tidak menemukan masalah yang berkaitan dengan pemalsuan koin atau hilangnya privasi transaksi secara langsung ketika menggunakan protokol Lelantus Spark. Akan tetapi, kami menemukan beberapa masalah dalam makalah itu sendiri. Hal ini telah dilaporkan langsung kepada penulis dan telah diperbaiki. Lebih lanjut, kami memberikan panduan mengenai detail implementasi dan bukti keamanan untuk makalah Lelantus Spark.

Kami mulai mengaudit versi 363b2597476663c5708b55f985b5130ab54898a8 dari makalah tersebut. Ketika kami menemukan masalah, kami langsung melaporkannya kepada penulis dan memperbarui versi yang kami tinjau.

2 Temuan

2.1 Definisi yang hilang dari $\{\sigma_i\}$ dalam Sistem Pembuktian Satu-Dari-Banyak yang Paralel

Dalam versi yang telah diaudit dari makalah Lelantus Spark, $\{\sigma_i\}$ tidak didefinisikan. Oleh karena itu, tidak mungkin untuk memverifikasi secara independen kebenaran dari konstruksi Sistem Pembuktian Paralel Satu-Dari-Banyak dan pembuktiannya.

Status: Penulis memperbarui notasi dan mengklarifikasi dari mana konstruksi berasal dalam versi 2156a2f152864bd1ffafcad5df36f78acce9e680.

2.2 Kondisi pada $\{a_{i,j}\}$ tidak ada pada Sistem Pembuktian Paralel Satu-Dari-Banyak

Istilah $\{a_{i,j}\}$ yang dipilih secara seragam secara acak oleh pembukti dalam Sistem Pembuktian Satu-Dari-Banyak secara paralel berasal dari *Cincin Akuntabel Pendek*

Tanda tangan dari DDH oleh Bootle dkk. Namun, dalam deskripsi yang disediakan di Lampiran B, tidak ada ketentuan tentang persyaratan $\{a\}_{i,j}$

Status: Penulis telah menambahkan kondisi tersebut dan sekarang dalam versi a9ec86451b37fd0e620067c4c1435b63feaac13f.

2.3 Pemeriksaan verifikasi di Sistem Penyediaan Satu Dari Banyak Paralel ada kesalahan

Langkah verifikasi ketiga dan keempat dalam Sistem Pembuktian Paralel Satu-Dari-Banyak tidak benar karena persamaan tidak lagi berlaku. Suku penjumlahan kedua di sisi kiri dari persamaan seharusnya merupakan suku hasil kali karena protokol menggunakan notasi aditif.

Status: Pemeriksaan verifikasi telah diubah pada versi 4ef12e8db9a799b1eef8122bda2f5498c927b560 dari makalah ini.

2.4 Jenis α_1 pada bukti Lemma 1 dari Lampiran C adalah salah

Pada Lemma 1 di Lampiran C yang digunakan untuk membuktikan bahwa sifat Keseimbangan berlaku untuk konstruksi Lelantus Spark, α_1 haruslah sebuah elemen dari $\mathbb{F}$ dan bukannya F, karena F adalah generator dari $\mathbb{F}$ dan bukannya sebuah himpunan.

Status: Hal ini telah diperbaiki dalam versi df9ee648ee26a2b5073c0946d873d7a9ef988782 dari makalah ini.

2.5 Lemma 1 dinyatakan untuk kedua jenis transaksi

Pada Lampiran C, pernyataan Lemma 1 tidak memperhitungkan bahwa koin yang berasal dari transaksi pencetakan ulang tidak memiliki label yang melekat padanya karena ini adalah koin baru. Pernyataan tersebut seharusnya secara eksplisit menyatakan bahwa lemma ini hanya berlaku untuk transaksi pembelanjaan.

Status: Hal ini telah diperbaiki dalam versi fc7dd6b10ed563e248a25778f2c02426dee6c94f dari makalah ini

2.6 Π_{rec} harus diuraikan secara eksplisit dalam identifikasi algoritma

Algoritma Identify mengambil input sebuah koin dan mengembalikan nilai dan memo yang dilampirkan kepada penerima atau entitas yang ditunjuk. Akan tetapi, pada langkah 2, pada saat mem-parsing koin untuk mendapatkan detail yang relevan, Π_r *ec*, bukti representasi untuk koin tersebut, tidak ada. Dengan demikian, Langkah 5 tidak dapat diselesaikan.

Status: Ini telah diperbaiki pada versi 8217abd24fdf9ab787a74bd5f334c3e4564e7608.

2.7 Kesalahan ketik

Ada beberapa kesalahan ketik yang kami identifikasi dalam makalah ini.

1. Pada halaman 35, weather seharusnya whether

2. Pada halaman 35, L-IND seharusnya LIND.

Status: Ini telah diperbaiki sejak 4a627cd41ae3fb577ceb3d6bf32f4ed280da1d69

2.8 S dikenal sebagai komitmen nomor seri tetapi juga disebut kunci publik koin

Dalam makalah ini, istilah *komitmen nomor seri* dan *kunci publik koin* digunakan secara bergantian. Hal ini dapat menyebabkan kebingungan karena komitmen dan kunci publik berbeda dalam kriptografi.

Status: Ini telah diperbaiki sejak f5fe7bc16d61a6ac2ff94207e2fc292401b2314e

2.9 Parameter dari langkah RepVerify algoritma Identify didefinisikan di Lampiran D tetapi tidak di dalam makalah itu sendiri

Untuk meningkatkan kejelasan ketika membaca deskripsi algoritma untuk Identify, akan lebih baik untuk mengklarifikasi bahwa input untuk pemeriksaan **RepVerify** pada langkah 5 adalah hasil dari fakta bahwa setelah memverifikasi Π_{rec} pada K_{div} , kita mendapatkan identitas bahwa $K = K$.

Status: Tidak diperbaiki.

2.10 Verifikasi bukti pengetahuan tentang kunci mutlisignature gagal

Pada bagian 5.1, selama pembuatan kunci multisig baru, pada langkah 6, kita memeriksa bahwa bukti pengetahuan dari langkah 3 valid setelah menerima (R_β , μ_β , C_β , $s_{1,\beta}$, $s_{2,\beta}$). Kondisi pada Langkah 6.b tidak menghasilkan penyelesaian verifikasi yang sukses, karena kita mendapatkan yang berikut ini

$$\mu_\beta G - \vdash_{pok} (\beta, C_{\beta,0} , R_\beta) = k_\beta G + \vdash_{pok} (\beta, a_{\beta,0} G, R_\beta)[a_{\beta,0} G - 1] \neq R_\beta$$

Status: Hal ini telah diperbaiki dalam versi c1ea7033aafc20c3f4b1def9d2a42f0453dbc3fd dari makalah ini.

3 Komentar Umum

3.1 Kutipan untuk konstruksi kriptografi yang dipesan lebih dahulu

Terdapat beberapa konstruksi dalam makalah ini yang merupakan modifikasi dari protokol kriptografi yang sudah dikenal. Sebaiknya juga mengutip makalah asli yang menghasilkan konstruksi ini untuk kelengkapan.

3.2 Semua protokol harus non-interaktif menggunakan Fiat- Shamir Transform

Untuk membantu pembuktian keamanan secara teoritis, penulis telah menulis semua protokol di dalam makalah ini secara interaktif. Akan tetapi, protokol-protokol ini perlu diimplementasikan secara non-interaktif menggunakan Fiat-Shamir Transform. Hal ini tidak dicatat dalam makalah. Karena mengubah protokol interaktif menjadi varian non-interaktif adalah masalah yang tidak sepele, hal ini harus dicatat dalam makalah.

3.3 Bukti Keamanan untuk Konstruksi Kriptografi yang Dipesan Lebih Dahulu

Ada beberapa konstruksi yang digunakan dalam pro- tocol Lelantus Spark yang dimodifikasi untuk digunakan dengan protokol. Dengan demikian, diasumsikan bahwa karena modifikasi ini sangat minim, maka tidak diperlukan bukti keamanan. Namun, secara historis, ini adalah area di mana bug kemudian muncul. Oleh karena itu, kami menyarankan agar bukti-bukti untuk konstruksi ini ditulis dengan hati-hati atau jika ada bukti di makalah lain untuk konstruksi ini, maka bukti tersebut harus dikutip. Secara khusus, konstruksi Paralel Satu-Dari-Banyak yang dijelaskan di Lampiran B harus memiliki bukti untuk membenarkan bahwa itu memang HVZK.

3.4 Rincian tentang Saluran Komunikasi

Dalam banyak protokol yang menjaga privasi, ada asumsi yang dibuat tentang bagaimana informasi dikirim di antara berbagai aktor dalam protokol. Namun, tidak ada pembahasan seperti itu dalam audit Lelantus Spark. Bagaimana informasi tertentu dalam protokol dikomunikasikan dapat memengaruhi jaminan privasi protokol ketika diterapkan dalam praktik. Karena aplikasi praktis dari makalah ini, kami merekomendasikan diskusi singkat tentang bagaimana pilihan saluran komunikasi mempengaruhi Lelantus Spark.