Audit Kriptografi Lelantus

Dmitry Khovratovich dan Ilya Kizhvatov

ABDK.Consulting

September 2020

1 Pendahuluan

Kebanyakan mata uang digital yang bertujuan untuk menjaga kerahasiaan pengirim dan penerima, melakukannya dengan menyembunyikan asal-usul transaksi di antara banyak koin yang tidak terpakai (dalam model UTXO) atau di antara semua akun yang memungkinkan. Lelan- tus [Jiv19] adalah sebuah protokol untuk pengaturan yang pertama. Sebuah koin direpresentasikan sebagai sebuah komitmen homomorfis dengan nilai nominal dan rahasianya, sehingga seseorang dapat membuktikan kepemilikan sebuah koin dengan membuktikan pengetahuan tentang pembukaan komitmen. Untuk menyembunyikan koin tertentu yang ingin dibelanjakan, Lelantus mengeksploitasi protokol *one-out-of-many yang telah* dimodifikasi [GK15; BCC+15]. Keuntungan besar dari Lelantus dibandingkan protokol yang berorientasi pada privasi lainnya adalah kinerjanya yang masuk akal (ukuran bukti logaritmik dan waktu pembuktian dalam 2 detik untuk 2 set anonimitas berukuran^{16} -size) dan tidak memerlukan pengaturan yang terpercaya seperti pada mata uang digital seperti Zcash [Zca] yang harus menggunakan fungsi hash khusus untuk hal ini.

Lelantus telah diterbitkan pada tahun 2019 dan telah menarik cukup banyak perhatian di masyarakat. Beberapa[1] protokol mata uang kripto[2] mengumumkan transisi ke Lelantus untuk meningkatkan privasi.

Tim Zcoin telah meminta kami untuk meninjau makalah kriptografi yang secara resmi mendeskripsikan Lelantus dan memberikan bukti keamanannya. Kami telah mengidentifikasi satu masalah utama yang muncul dari penggunaan yang salah dari protokol satu-dari-banyak yang dimodifikasi. Konkritnya, belum terbukti bahwa bagian dari transkrip memiliki bentuk khusus, dan hal ini dapat dieksploitasi oleh musuh untuk menghasilkan koin palsu. Kami telah menyarankan solusi yang mungkin dalam laporan. Kami telah menyarankan beberapa cara untuk memperbaiki bukti keamanan.

Kami juga telah mengidentifikasi beberapa masalah dalam bukti keamanan yang perlu diklarifikasi tetapi tampaknya tidak terlalu penting bagi keamanan.

Masalah kritis dan beberapa masalah yang tidak terlalu parah telah diperbaiki pada versi berikutnya dari makalah yang telah kami ulas. Di bawah ini kami memberikan penjelasan rinci tentang bug dan masalah lainnya.

2 Memperbaiki Masalah Kritis

2.1 Detail Protokol

Dalam Lelantus, semua koin adalah multikomitmen Pedersen dengan bentuk keacakan $gsecretf^{value}$ di mana hasil kali dari dua komponen pertama dapat dilihat sebagai kunci publik pemilik Q. Seorang pemilik dapat MEMBELANJAKAN koin-koin $I_1, I_2, \ldots, I_s$ dengan membuat koin keluaran $O_1, O_2, \ldots O_t$ dengan bentuk yang sama disertai dengan hal-hal berikut ini (detailnya penting untuk serangan):

- *Enkripsi* nilai yang dikomitmenkan pada kunci publik penerima dan pembuatan bukti rentang pada nilai nominal koin keluaran.
- *Bukti kepemilikan* : tentukan himpunan anonimitas koin C yang harus mencakup koin masukan diantara banyak koin lainnya. Untuk setiap koin input I_j dengan rahasia s_j membangun sebuah bukti π_j bahwa jika kita secara homomorfis mengurangkan g^s j dari semua koin di C maka

himpunan yang dihasilkan berisi komitmen ke nol rahasia, dengan demikian membuktikan bahwa kita memiliki beberapa koin di C. Pembuktian ini merupakan modifikasi dari [BCC+15] dengan tambahan utama bahwa transkrip tersebut juga berisi nilai-nilai tertentu $\{G_k\}$ dan $\{H_k\}$, dimana kita buktikan bahwa nilai-nilai ini akan dikalikan dengan komitmen ke 0.

[1] https://zcoin.io/lelantus-zcoin/

[2] https://beam.mw/

- *Bukti Saldo* : membangun sebuah bukti π_{balance} bahwa nilai gabungan dari koin keluaran sama dengan nilai koin masukan. Untuk ini buktikan bahwa hasil kali koin keluaran dibagi dengan hasil kali G_k adalah koin yang valid dengan nilai nominal nol. Untuk pasangan koin keluaran dan masukan tunggal O_1 , I_1 , yang cukup bagi kita, persamaannya terlihat sebagaiberikut:

$$\frac{1}{\prod_k G_k^{x^k}} \stackrel{?}{=} Q\, f^{\alpha\beta}$$

  dimana *x* adalah tantangan Fiat-Shamir dari bukti kepemilikan, *Q* adalah kunci publik penerima (setara dengan koin bernilai nol) dan *α, β* adalah logaritma diskrit yang kita buktikan dengan pengetahuan.

Para perancang protokol menyediakan dua bukti keamanan untuk protokol tersebut:

- Bahwa bukti kepemilikan koin tersebut adalah bukti yang kuat, lengkap, dan tanpa pengetahuan.
- Bahwa bukti saldo itu lengkap, sehat, dan tanpa pengetahuan.

Ini (bersama dengan sifat-sifat dari bukti-bukti lainnya) mengimplikasikan kebenaran dari operasi Spend.

2.2 The Bug

Masalah dari protokol yang dijelaskan di atas adalah bahwa keamanan bukti saldo terbukti dengan asumsi bahwa G_k yang digunakan oleh pembukti terbentuk dengan benar. **Akan tetapi, kondisi ini tidak benar-benar terbukti pada bukti kepemilikan koin!** Memang, bukti kepemilikan koin mengimplikasikan pengetahuan akan rahasia koin tetapi tidak secara otomatis mengimplikasikan kebenaran transkrip. Kami telah mampu mengeksploitasi hal ini dan tampaknya menciptakan koin secara tiba-tiba.

Konkritnya, misalkan kita membelanjakan sebuah koin *I dengan* nilai *v,* kemudian dalam bukti kepemilikan kita membuat G_0 , H_0 yang dimodifikasi yang kita tunjukkan dengan $G\tilde{}0$, $H\tilde{}0$:

$$G\tilde{}0 = G_0 - h^{\xi} \tag{1}$$

$$H\tilde{}0 = H_0 - h^{-\xi} \tag{2}$$

agar produk mereka tidak berubah.

Prover kemudian menghasilkan beberapa tantangan Fiat-Shamir *x*, yang bergantung pada $G\tilde{}0$.

Kemudian, sebagai ganti koin O dengan nilai nominal *v*, kita membuat koin keluaran $O = O - {}^{hxm}$ dengan nilai $v + {}_{xm}$. Hasilnya, bukti kebenaran keseimbangan berlaku:

$$\frac{O\tilde{}xm}{\prod_k G\tilde{}x_k^k} = \frac{Oxm}{h^{\xi}} \frac{h^{\frac{xm\xi}{xm}}}{\prod_k G_k^{xk}} = \frac{O^{xm}}{\prod_k G_k^{xk}} = Q f^{\alpha\beta}.$$

Dengan demikian kami telah menciptakan $_{xm}$ nilai. koin yang memiliki ekstra $^{\xi}$

Untuk melakukan hal di atas, prover jahat mengeksekusi langkah 6 dari algoritma **Spend** sebelum langkah 3. Hal ini dimungkinkan karena langkah 6 tidak bergantung pada langkah-langkah sebelumnya.

Hal ini mengindikasikan sebuah masalah pada teorema keamanan protokol (Lampiran A.B, halaman 15-16). Tampaknya hal ini mengasumsikan bahwa jika properti saldo transaksi tidak berlaku maka bukti saldo transaksi juga gagal. Alasan ini cacat karena secara implisit mengasumsikan bahwa G_k dibentuk dengan benar, yang mana kami tunjukkan mungkin tidak benar.

Sebuah bukti representasi untuk semua nilai G_k tidak akan cukup karena $_{G\tilde{}k}$ juga melewatinya:

$$G_k = h^{\rho}\, k\, f^{\gamma k + \tau k} \tag{3}$$

$$_{G\tilde{}k} = h^{\rho}\, k\text{-}\nu f^{\gamma k + \tau k} \tag{4}$$

(5)

Kami mencatat bahwa nilai G_k dan Q_k dapat dimodifikasi dengan berbagai cara, satu-satunya syarat adalah produknya tetap sama.

2.3 Perbaikan

Penulis Lelantus memodifikasi bukti tersebut dengan menambahkan koin keluaran ke dalam transkrip protokol yang digunakan ketika membuat tantangan x, dan memperbaiki bagian lain dari bukti tersebut.

Kami tidak menemukan masalah pada bukti yang baru.

2.4 Perbaikan lain yang mungkin dilakukan

Mungkin lebih baik untuk menjelaskan dalam bentuk interaktif terlebih dahulu, di mana subprotokol jangkauan, kepemilikan, dan keseimbangan adalah bagian dari yang besar. Kemudian buktikan kebenaran dari versi interaktif dengan menggunakan teknik rewinding. Terakhir, kompilasi protokol menjadi protokol non-interaktif dengan menerapkan transformasi Fiat-Shamir berkali-kali.

3 Memperbaiki Masalah Sedang

- Lampiran A.A, Halaman 14, baris 75: tidak terbukti secara formal bahwa C memiliki bentuk ini. Mungkin dapat diturunkan dari bukti kesehatan untuk transaksi SPEND. Hal yang sama untuk baris 79. *Penjelasan telah ditambahkan*.
- Lampiran A.A, Halaman 14, baris 85-105: Pembuktiannya tidak ketat. Sebuah bukti biasa dari jenis ini akan menunjukkan bahwa sebuah lawan yang berhasil dapat menghasilkan S, x, atau s, atau kita dapat mengekstrak nilai-nilai ini dari lawan tersebut. *Pembuktian telah dimodifikasi.*
- Kondisi 4: ketidaksetaraan keseimbangan tidak secara langsung menyiratkan eksponen non-nol dalam A/B. Harus ada bukti kesehatan dari protokol keseimbangan yang akan mengimplikasikan hal tersebut. *Bukti telah* dimodifikasi.
- Lampiran A.B, Halaman 15, baris 6-8: Harus dijelaskan mengapa parameter koin keluaran yang dituduhkan dianggap sebagai bagian dari saksi. Mungkin hal ini mengikuti struktur dari range proof; jika tidak, maka tidak mudah untuk membuktikan bahwa koin keluaran memiliki format tertentu.

Beberapa kesalahan ketik telah ditemukan dan diperbaiki.

4 Isu-isu Kecil yang Tersisa

Kertas asli:

- Halaman 7: Pada paragraf properti **Saldo,** tidak jelas bagaimana tepatnya jumlah koin yang dikirim dari satu alamat ke alamat lain didefinisikan. Apakah kita mengaitkan dengan setiap Pengeluaran sebuah daftar eksplisit dari alamat input dan output? Bagaimana cara menangani alamat siluman? Bagaimana kita menjamin bahwa semua koin yang diterima oleh buku besar memiliki alamat yang dapat diidentifikasi dengan jelas?
- Halaman 7: Pada paragraf **Ledger Indistinguishability**, akan lebih baik untuk memberikan bentuk eksplisit dari transaksi yang dikirim ke salah satu buku besar, karena saat ini deskripsinya tidak ketat.
- Halaman 8, Algoritma pengaturan: Pengaturan... tidak didefinisikan; tidak jelas apa yang dimaksud dengan *bp* dan *rp* (anti peluru dan bukti jangkauan?).
- Halaman 9, dalam deskripsi teks bukti ooom: $\sigma_{l,i}$ notasi membingungkan dengan tanda tangan, pertimbangkan untuk menggunakan $\delta_{l,i}$
  sebagai gantinya.
- Halaman 9, baris 59: g^{y} seharusnya fk^{y}
- Halaman 9, Gambar 2:
  - Protokol ini tidak secara jelas merinci pernyataan bahwa hal itu terbukti;
  - Di tengah, iterasi pada j tidak sejajar ke kiri.
  - Semua Z_q haruslah Z_p .
- Halaman 10, kebingungan antara Q_i dari alamat pribadi dan Q_k pada Gbr. 2; pertimbangkan untuk mengganti nama
  Q_k 's pada Gbr. 2 karena mereka tetap hanya digunakan secara internal dalam bukti ooom.

- Halaman 10, baris 17: π_{range} di sini memiliki 3 parameter, bukan 4 (rentang tidak dilewati)
- Halaman 11: deskripsi protokol saldo transaksi mencampuradukkan kelengkapan dan bukti kesehatan di dalamnya. Sebagai gantinya, seseorang harus menyediakan algoritma dan kemudian secara eksplisit membuktikan kelengkapan, dan kemudian merujuk ke Lampiran C untuk kesehatan.

- Halaman 11, baris 43: penyebut harus $g\,k^{sn}$
- Halaman 11, baris 65: h seharusnya adalah f.
- Halaman 13, paragraf pertama dari bagian tersebut: Z_P seharusnya Z_p.
- Halaman 13, paragraf kedua baris ketiga: nomor gambar hilang.
- Halaman 14, akhir paragraf pertama: tidak dijamin bahwa nomor seri adalah unik. Mungkin skema ini sudah lengkap dengan asumsi demikian.
- Halaman 15, baris 53-56. Tidak jelas mengapa 5 kondisi ini mengimplikasikan pertidaksamaan. Apakah mungkin untuk mengaitkan bagian dari pertidaksamaan dengan setiap kondisi?
- Halaman 16, baris 38-41: mungkin cukup untuk menunjukkan bahwa lawan yang melanggar kondisi 5 dapat menghasilkan (s, v, r), kemudian berargumen bahwa transaksi pengeluaran oleh pihak-pihak yang jujur tidak mengungkapkan hal t e r s e b u t karena sifat zero-knowledge dari ooom-proof.
- Halaman 18: alih-alih G_k seharusnya ada $(G_k - Q)_k^{-1}$, dan kemudian baris terakhir protokol ditulis ulang sebagai

$$c^{(e)} - \sum_{k=0}^{n} (G_k - T^{(e)} = Comm(0, z_e, z_e)$$

Makalah yang diperbarui:

- Halaman 19: w.r.t pemulihan $v^o_1, \ldots, v^o_{baru}$, mungkin saksi tidak boleh menyertakan orang-orang ini nilainya tetapi hanya jumlahnya saja?
- Halaman 19: persamaan (4) dan persamaan-persamaan berikut: R^l seharusnya menjadi R^i
- Halaman 20: Anda dapat mengekstrak nilai koin yang terpisah jika range prover juga dicakup oleh simulator.

Referensi

[BCC+15] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, dkk. "Tanda Tangan Cincin Pendek yang Dapat Dipertanggungjawabkan Berdasarkan DDH". In: *ESORICS (1)*. Vol. 9326. Catatan Kuliah dalam Ilmu Komputer. Springer, 2015, hal. 243-265 (cit. pada hal. 1).

[GK15] Jens Groth dan Markulf Kohlweiss. "Satu-Dari-Banyak-Bukti: Atau Bagaimana Membocorkan Rahasia dan Menghabiskan Koin". Dalam: *EUROCRYPT (2)*. Vol. 9057. Catatan Kuliah dalam Ilmu Komputer. Springer, 2015, hal. 253-280 (cit. pada hal. 1).

[Jiv19] Aram Jivanyan. "Lelantus: Menuju Kerahasiaan dan Anonimitas Transaksi Blockchain dari Asumsi Standar". Dalam: *IACR Cryptol. ePrint Arch.* 2019 (2019), hal. 373 (cit. pada hal. 1).

[Zca] *Spesifikasi protokol ZCash.* https://github.com/zcash/zips/blob/master/protocol/protokol.pdf. 2020 (dikutip dari hal. 1).