Laporan Akhir Audit Lelantus Spark

Linfeng (Daniel) Zhou

Jan 2022

1 Pendahuluan

Lelantus Spark adalah protokol yang memodifikasi protokol Lelantus untuk memberikan privasi penerima, fitur keamanan yang lebih baik, dan fitur kegunaan tambahan. Saya mulai mengaudit makalah ini ketika tim Firo terus memperbarui protokol Lelantus Spark. Laporan ini mengaudit versi yang telah dipublikasikan di IACR eprint - https://eprint.iacr.org/2021/1173. Saya telah menggali detail dari makalah tersebut. Tidak ada masalah keamanan kritis yang ditemukan tetapi saya menemukan beberapa masalah yang tercantum dalam laporan ini di bawah ini.

2 Temuan

2.1 Definisi yang hilang untuk kelengkapan, kesehatan khusus, dan pemeriksa kejujuran khusus tidak ada pengetahuan tentang sistem pembuktian

Protokol Lelantus Spark membutuhkan penggunaan sistem pembuktian representasi, sistem pembuktian Chaum-Pedersen yang dimodifikasi, sistem pembuktian paralel satu-dari-banyak dan semua sistem pembuktian ini harus memenuhi kelengkapan, pengetahuan nol pemverifikasi khusus dan sifat-sifat kesehatan khusus. Akan tetapi, makalah ini tidak memiliki definisi keamanan formal dari sifat-sifat penting ini. Karena definisi-definisi ini penting, terutama dalam pembuktian keamanan seperti yang dijelaskan di Lampiran, saya menyarankan untuk menambahkan definisi formal dari sifat-sifat ini. Sebagai contoh,

1. *Kelengkapan*. Jika $(x, w) \in \mathrm{R}$ maka semua transkrip 3 langkah yang jujur untuk (x, w) dapat diterima.

2. *Kebaikan Khusus*. Ada sebuah algoritma yang efisien Ext yang, dengan input x dan sebuah kolinier untuk x, menghasilkan sebuah saksi w sedemikian sehingga $(x, w) \in \mathrm{R}$.

3. *Special Honest Verifier Zero Knowledge (SHVZK)*. Ada simulator PPT Sim yang mengambil input $x \in L_R$, parameter keamanan 1^λ dan $c \in \{0, 1\}^\ell$ dan mengeluarkan output

menerima transkrip untuk x di mana c adalah tantangannya. Selain itu, untuk semua string ℓ-bit$c$, distribusi output dari simulator pada input (x, c) secara komputasi tidak dapat dibedakan dari distribusi transkrip yang jujur yang diperoleh ketika V mengirimkan c sebagai tantangan dan P berjalan pada input umum x dan input pribadi w sedemikian sehingga $(x, w) \in \mathrm{R}$. Kita mengatakan bahwa Π sempurna ketika kedua distribusi tersebut identik.

Perhatikan bahwa hal di atas hanyalah sebuah contoh, makalah ini mungkin perlu menambahkan definisi yang sedikit berbeda untuk memenuhi persyaratan.

2.2 Ketidaksesuaian antara elemen output serta output yang ditentukan di CreateCoin

Pada bagian 4.4, algoritma **CreateCoin** didefinisikan untuk menghasilkan sebuah nomor seri kom- mitmen S, sebuah kunci pemulihan K, komitmen nilai C, bukti rentang komitmen nilai Π_{rp} (jika $b = 0$, nilai terenkripsi v (jika $b = 0$) atau nilai v (jika $b = 1$), memo terenkripsi m. Akan tetapi, pada langkah 9, algoritma mengeluarkan tuple $(S, K, C, \Pi_{rp}, \Pi_{rec}, v, m)$ jika $b = 0$, atau mengeluarkan $(S, K, C, \Pi_{rec}, v, m)$ jika $b = 1$. Kita perlu membuang Π_{rec} pada output karena sepertinya tidak digunakan pada algoritma lain atau mendefinisikan ulang output dari **CreateCoin.**

Sebagai umpan balik dari tim Firo, bukti Π_{rec} digunakan dalam algoritma **Identify** dan masalah ini telah diperbaiki dalam versi berikut.

2.3 Π_{chaum} harus menjadi bukti independen dalam output dari Spend trans- action

Dalam algoritma **Pengeluaran**, algoritme ini menghasilkan transaksi pengeluaran

$$\mathsf{tx}_{spend} = (\mathsf{InCoins}, \mathsf{OutCoins}, f, \{S'_u, C'_u, T_u, (\Pi)_{par}, \Pi\})_{chaum}{}_{u=0}^{w-1}$$

tetapi Π_{chaum} adalah sebuah bukti yang dihitung secara independen, jadi ia harus menjadi sebuah elemen independen di dalam keluaran, bukan di dalam setiap tuple.

Sebagai umpan balik dari tim Firo, masalah ini telah diperbaiki pada versi berikutnya.

2.4 Penerima tidak boleh mengetahui $d_{\beta,k}$ dan $e_{\beta,k}$ di Bagian 6.2, PreCompute

Pada bagian 6.2, algoritma **PreCompute**, langkah 2 menjelaskan bahwa pada saat menerima vektor L_β dari pemain lain β, periksa bahwa $d_{\beta,k}\ \mathrm{G} \neq 0$ dan $e_{\beta,k}\ \mathrm{G} \neq 0$ untuk semua k. Akan tetapi, $d_{\beta,k}$ dan $e_{\beta,k}$ haruslah nilai privat pihak β dan pihak α tidak dapat mengetahuinya. Juga, karena $d_{\beta,k}\ \mathrm{G}$ dan $e_{\beta,k}\ \mathrm{G}$ adalah nilai grup, kita tidak dapat memeriksa $\neq 0$. Dengan demikian, cara terbaik untuk menjelaskan hal ini adalah pihak α pertama-tama menguraikan setiap $L_{\alpha,k} = (D_{\beta,k}, E_{\beta,k})$ dan memeriksa $D_{\beta,k}$ dan $E_{\beta,k}$ tidak generator grup.

Saya berdiskusi dengan tim Firo dan pada dasarnya ini adalah masalah notasi, yang dapat menyesatkan pembaca yang salah memahami makalah ini dan kami sepakat untuk membuat notasi yang lebih jelas dalam versi berikutnya.

2.5 Menambahkan tabel perbandingan yang membandingkan Lelantus Spark dengan karya-karya lain yang serupa

Pada bagian 7, makalah ini menyajikan tabel untuk menunjukkan efisiensi Lelantus Spark. Untuk menunjukkan keunggulan efisiensi dari Lelantus Spark, akan lebih baik jika menambahkan tabel untuk mencantumkan semua karya yang serupa dan membandingkan ukuran nilai yang sesuai di setiap kolom. Jika kami dapat menunjukkan bahwa Lelantus Spark menyediakan lebih banyak fitur keamanan dan juga memberikan efisiensi yang baik, ini akan menjadi sinyal yang baik dan ini bermanfaat bagi makalah ini untuk dapat diterima.

Tim Firo setuju untuk menambahkan tabel perbandingan seperti itu di versi berikutnya.

2.6 Menyalahgunakan fungsi komitmen Com di Lampiran B

Pada Lampiran B, makalah ini menggunakan $\mathsf{Com}(\text{-}, \text{-})$ dengan tidak benar. Sebagai contoh, $A = \mathsf{Com}(\{a\}_{j,i}^{m-1,n-1}, r)$. $\sum_{j=0}^{i-1}$ $_A$
Akan tetapi, Com hanya mengambil dua nilai sebagai input, satu adalah nilai komitmen, satu lagi adalah ran- domness, hal ini membingungkan pembaca, sehingga perlu diubah menjadi $\mathsf{Com}(a_{j,i}, r_A)$ untuk semua $0 \le j \le m - 1$ dan $0 \le i \le n - 1$. Ada juga banyak tempat lain yang menyalahgunakannya dalam hal ini
bagian, sehingga membutuhkan perubahan yang signifikan.

2.7 Kurangnya deskripsi mengenai modifikasi definisi keamanan sistem pembayaran

Pada Lampiran C, makalah tersebut menyebutkan bahwa "kami secara resmi membuktikan keamanan Spark dalam model keamanan yang terkait (tetapi dimodifikasi); pembuktiannya mengikuti cara yang mirip dengan yang ada pada [3]. " Akan tetapi, tidak jelas apa yang dimaksud dengan modifikasi tersebut. Kita perlu menambahkan konteks untuk menyoroti model keamanan yang dimodifikasi dan properti keamanan apa yang harus dicapai.

Kami telah mendiskusikan masalah ini dan setuju bahwa kami telah mendefinisikan model keamanan, tetapi masih kurang mempertimbangkan kueri CreateCoin, Identify, Recover dalam model keamanan. Tim Firo akan menambahkan lebih banyak detail tentang hal ini.

2.8 Ketidaksesuaian dalam definisi sistem DAP

Pada bagian 3, ketika makalah ini memperkenalkan definisi sistem DAP, makalah ini berisi al-goritma

Setup, CreateKeys, CreateAddress, CreateCoin,Mint, Identify, Recover, Spend, Verify

tetapi dalam lampiran C didefinisikan sebagai

$$\Pi = (\textbf{Setup, CreateAddress,Mint,Mint, Spend, Recover, Verify})$$

Pasti ada beberapa perbedaan antara protokol Lelantus Spark dan sistem DAP yang asli. Kita harus mendefinisikan sistem DAP kita sendiri (mungkin Lelantus Spark mencapai sistem DAP yang lebih kuat) dan membuktikan bahwa semua algoritma bersama-sama mencapai keamanan sistem pembayaran.

Tim Firo akan memperbaiki masalah ini di versi berikutnya.

3 Komentar Kecil dan Kesalahan Ketik

- Pada bagian 2.5, karena keamanan IND-CCA2 mengimplikasikan keamanan IND-CPA, mungkin kita tidak perlu menyebutkan IND-CPA.
- Langkah 3 dari algoritma **Recover** melewatkan input λ dan *pp*, seharusnya

  Identifikasi (λ, *pp*, addr_{in} , Coin, AddrTable)

- Pada Bagian 5 Algoritma **CreateKeys,** $C_{\beta,j}$ berarti elemen ke-j dari C_β yang diterima dari pemain β, tetapi tidak ada penjelasan mengenai notasi tersebut. Perlu ditambahkan beberapa kalimat untuk menjelaskan notasi tersebut.
- Karena kami menggunakan sistem pembuktian satu-keluar-dari-banyak paralel sebagai blok bangunan yang penting, mungkin ada baiknya mempertimbangkan untuk menggunakan sistem pembuktian banyak-keluar-dari-banyak https://eprint.iacr.org/2020/293 dan pelajari apakah sistem ini memiliki lebih banyak keuntungan.
- Pada Lampiran B, tambahkan kutipan untuk fungsi delta Kronecker dan jelaskan apa itu fungsi delta Kronecker.

Tim Firo setuju untuk memperbaikinya di versi berikutnya.