Mengaktifkan Pembayaran Anonim yang Tidak Dapat Dilacak dalam Protokol Lelantus

Aram Jivanyan[1] and Sarang Noether[2]

[1] Zcoin
aram@zcoin.io
https://zcoin.io
[2] Monero Research Lab
sarang.noether@protonmail.com
https://getmonero.org

Abstrak. Kami menyediakan pembaruan pada protokol Lelantus untuk memungkinkan pembayaran anonim langsung yang tidak dapat dilacak.

Kata Kunci: Lelantus, One-out-of-Many Proofs, Double-blinded commitments

1 Perkenalan

Salah satu isu utama dari protokol Lelantus [3] adalah ketertelusuran dalam transfer anonim langsung. Dalam skenario tersebut, pengirim dapat mengamati transaksi dan mendeteksi ketika sebuah koin (yang direpresentasikan sebagai sebuah komitmen) dibelanjakan oleh penerima. Karena hal ini menimbulkan masalah keamanan yang penting, salah satu solusinya adalah dengan mengharuskan penerima untuk membelanjakan koin yang baru saja diterima dan mencetak koin baru untuk dirinya sendiri untuk menghilangkan pelacakan ini. Walaupun pendekatan ini dapat mengurangi masalah ketertelusuran, pendekatan ini membutuhkan sebuah transaksi tambahan, meningkatkan ruang yang dibutuhkan pada blockchain, waktu verifikasi secara keseluruhan, dan penundaan sebelum koin dapat digunakan. Pendekatan ini juga dapat memperkenalkan data waktu yang dapat digunakan oleh pengamat untuk membentuk heuristik tentang perilaku pengeluaran dan mengurangi anonimitas praktis.

Kami menjelaskan peningkatan protokol yang dimaksudkan untuk mengurangi masalah ini dengan cara yang lebih cerdas dan aman.

2 Latar Belakang

Untuk mendukung peningkatan protokol ini, kita harus memodifikasi bagaimana nomor seri koin Lelantus dihasilkan. Selanjutnya kita akan menggunakan bukti kriptografi representasi seperti yang dijelaskan di bawah ini.

2.1 Nomor Seri Koin dan Kunci Pembelanjaan

Di Lelantus, koin diwakili oleh komitmen buta ganda dalam bentuk $C = g^S h_1^V h_2^R$ dalam kelompok orde utama G.
Di sini S adalah nomor seri koin yang dihasilkan oleh hashing kunci publik yang unik $Q = g^q$, V adalah nilai koin, dan R adalah Pedersen blinder. Selama transaksi pembelanjaan, kunci publik koin Q diungkapkan untuk menghitung nomor seri S, yang dipublikasikan sebagai bagian dari transaksi; selanjutnya, pembelanja menandatangani seluruh transaksi dengan q untuk membuktikan kepemilikan koin. Kunci publik Q memungkinkan semua partisipan jaringan untuk menghitung nomor seri (yang dibutuhkan untuk verifikasi transaksi pembelanjaan) dan memverifikasi tanda tangan transaksi. Hal ini mencegah serangan pembakaran yang telah diketahui sebelumnya di mana penyusup jahat yang mengendalikan pesan jaringan dapat mencegat pembelanjaan yang jujur, mencetak koin dengan nomor seri yang sama, dan membelanjakannya [5]; dalam konstruksi kami, penyerang tidak akan dapat menandatangani dengan q, dan upaya pembakaran akan ditolak oleh jaringan. Perhatikan bahwa pada protokol Zerocoin yang asli, situasi ini tidak muncul karena protokol tersebut tidak mendukung transfer anonim secara langsung [4]. Masalah penelusuran muncul dalam kasus pembayaran langsung, di mana pertukaran Diffie-Hellman digunakan untuk menghasilkan Q. Pertukaran ini memastikan bahwa penerima, dan bukan pengirim, dapat memulihkan kunci privat q yang sesuai dengan koin. Akan tetapi, karena pengirim mengetahui public key Q, ia dapat mengamati transaksi sampai ia melihat public key ini kemudian diungkap dalam transaksi lain. Pada titik ini, pengirim mengetahui bahwa koin tersebut telah dibelanjakan. Perhatikan bahwa dalam

protokol Zerocoin yang asli, situasi ini tidak muncul karena protokol ini tidak mendukung transfer anonim secara langsung [4].

Kami mengusulkan untuk memodifikasi skema ini dan menentukan ulang nomor seri. Dengan menggunakan format komitmen yang sama, kami mempertimbangkan g^S menjadi nomor seri, di mana pembelanja sekarang harus menandatangani transaksi dengan *S* secara langsung. Selama transaksi pembelanjaan, g^S diungkapkan secara publik dan digunakan untuk memverifikasi tanda tangan transaksi.

Penting untuk disebutkan bahwa memungkinkan verifikasi batch yang efisien dengan menggunakan konstruksi ini masih memungkinkan.

2.2 Bukti Pengetahuan tentang Representasi

Perhatikan sebuah grup G berorde prima p dan n generator $g_1, g_2, \ldots, g_n$. Representasi elemen z terhadap z against the generator $g_1, g_2, \ldots, g_n$ adalah vektor $(s_1, s_2, \ldots, s_n)$ sedemikian hingga $z = g_1^{s_1} g_2^{s_2} \cdots g_n^{s_n}$. Di bawah ini kami jelaskan protokol untuk ukti representasi untuk nilai sembarang n, yang disebut sebagai bukti pengetahuan Schnorr yang digeneralisasi.

Secara formal, bukti representasi seperti itu adalah sebuah argumen tanpa pengetahuan untuk relasi berikut:

$$R = \{g_1, g_2, \ldots, g_n \in G, y \quad ; \quad s_1, s_2, \ldots, s_n \in Z_p \quad | \quad y = g_1^{s_1} g_2^{s_2} \cdots g_n^{s_n}\}$$

Protokol ini digambarkan pada Gambar 1. Memverifikasi kelengkapan protokol ini sangatlah mudah. Protokol ini dapat dikonversi menjadi protokol non-interaktif yang aman dan khusus honest-verifier zero-knowledge dalam model oracle acak menggunakan heuristik Fiat-Shamir [1].

$\text{Prover}(g_1, g_2, \ldots, g_n, y, (s_1, s_2, \ldots, s_n))$		$\text{Verifier}(g_1, g_2, \ldots, g_n, y)$
Computes		
$x_1, x_2, \ldots, x_n, \leftarrow_R \mathbb{Z}_p$	u	
$u = g_1^{x_1} g_2^{x_2} \ldots g_n^{x_n} \in G$	$\longrightarrow$	
	$\xleftarrow{x \leftarrow \{0,1\}^\lambda}$	
$t_1 = x_1 - x \cdot s_1 \in \mathbb{Z}_p$		
$t_2 = x_2 - x \cdot s_2 \in \mathbb{Z}_p$		
$\vdots$		
$t_n = x_n - x \cdot s_n$	$\xrightarrow{s_1, s_2, \ldots, s_n}$	Accepts if and only if $u = y^x g_1^{t_1} g_2^{t_2} \cdots g_n^{t_n}$

Gbr. 1. Bukti pengetahuan Schnorr yang digeneralisasi

3 Pembayaran Anonim Langsung

Untuk memastikan otentikasi yang tepat untuk pembelanjaan koin $C = g^S h_1^V h_2^R$, pemilik koin harus secara eksklusif memiliki nilai rahasia *S, V,* dan *R*. Sebuah transaksi pembelanjaan mengungkapkan nomor seri g^S dan memberikan tanda tangan yang valid menggunakan *S*. Tujuan kami adalah mengembangkan protokol yang memastikan bahwa hanya penerima yang dapat memulihkan *S* dan g^S , yang memastikan bahwa pengirim tidak dapat mengawasi nomor seri yang diketahui untuk melacak transaksi selanjutnya.

Pada Gambar 2 di bawah ini kami menjelaskan protokol tersebut. Perhatikan bahwa kami mengasumsikan bahwa penerima membuat alamat baru untuk setiap transaksi tersebut, dan bahwa pengirim diasumsikan mengirimkan nilai rahasia *y* dan *V* kepada penerima. Hal ini dapat dilakukan melalui saluran sisi aman, atau dengan mengenkripsi mereka dengan kunci publik penerima dan memasukkannya ke dalam transaksi.

Perhatikan juga persyaratan bagi penerima untuk menyertakan bukti Schnorr dari representasi titik Q sehubungan dengan generator g dan h2 ; tanpa ini, tidak mungkin untuk memverifikasi bahwa komitmen koin yang dihasilkan dibangun menggunakan generator publik tetap tanpa hubungan logaritma diskrit.

Pengirim		Penerima
		Sampel $x, r \leftarrow_R \mathbb{Z}_p$
		Menghitung alamat publik baru $Q = g^x h_2^r$
		Menghasilkan bukti Schnorr P pada titik Q
	Q, P ⟵	
Memverifikasi P		
Sampel $y \leftarrow_R \mathbb{Z}_p$		
Menciptakan koin output $C = Q^y h_1^V (= g^{xy} h_1^V h_2^{ry})$		
Menghasilkan bukti jangkauan sehubungan dengan generator Q dan h_1		
C, Q, P dipublikasikan ke blockchain	y, V ⟶	
		Mengungkap nomor seri koin g^{xy}
		Menghasilkan bukti Pembelanjaan untuk koin tersebut
		Menandatangani transaksi dengan kunci privat xy

Gbr. 2. Mencetak koin baru untuk penerima khusus

4 Menghasilkan Bukti Saldo

Konstruksi ini membutuhkan modifikasi dari proses pembuatan bukti saldo transaksi yang dijelaskan dalam [3]. Asumsikan sebuah transaksi menghabiskan N_{old} koin input dan output N_{new} koin $C_{O,1}, \ldots, C_{O,N_{new}}$. setiap koin output $C_{O,i}$ diasosiasikan dengan alamat Q_i, yang dipublikasikan pada blockchain dengan transaksi tersebut. Langkah-langkah pembuatan bukti saldo adalah sebagai berikut:

1. Pengirim mengambil semua koin keluaran, nilai keluaran bersih V_{OUT}, biaya transaksi f dan nilai tantangan umum value x ang digunakan untuk konstruksi Σ-proofs dan menghitung elemen berikut:

$$\begin{aligned}\mathbf{A} :&= (C_{O,1} \cdot \ldots \cdot C_{O,N_{new}})^{x^m} \cdot h_1^{(V_{OUT}+f)x^m} = \\ &= Q_1^{y_1 x^m} \ldots Q_{N_{new}}^{y_{N_{new}} x^m} h_1^{(V_{OUT}+V_{O,1}+\ldots+V_{O,N_{new}}+f)x^m}\end{aligned}$$

2. Mengambil elemen-elemen $z_{V1}, \ldots, z_{V_{N_{old}}}, z_{R1}, \ldots, z_{R_{N_{old}}}$ dan $\{Comm(0, \rho_k^t, \tau_k^t + \gamma_k^t)\}_{k=0}^{m-1}$ dari koresponding Σ-proof traskrip (untuk lebih jelasnya, mari merujuk pada makalah asli milik kami [3]) dan menghitung elemen:

$$\begin{aligned}\mathbf{B} :&= Comm(0; z_{V1} + \ldots + z_{VN_{old}}, z_{R1} + \ldots + z_{RN_{old}}) \cdot \prod_{t=1}^{N_{old}} \Big(\prod_{k=0}^{m-1} (h_2^{\gamma_k^t} \cdot Comm(0; \rho_k^t, \tau_k^t))^{x^k} \Big) \\ &= h_1^{(V_{I1}+\cdots V_{Iold})x^m} h_2^{\sum_{t=1}^{old}(R_{It} \cdot x^m + \sum_{k=0}^{m-1} \gamma_k^t \cdot x^k)}\end{aligned}$$

Jika saldo transaksi bertahan, eksponen h_1 pada A dan B akan dibatalkan:

$$\frac{\mathbf{A}}{\mathbf{B}} = Q_1^{y_1} Q_2^{y_2} \ldots Q_{N_{new}}^{y_{N_{new}}} h_2^Y \tag{1}$$

dimana

$$Y = -\sum_{t=1}^{old}\Big(R_{It}\cdot x^m + \sum_{k=0}^{m-1}\gamma_k^t\cdot x^k\Big)$$

Sekarang amati bahwa untuk memberikan bukti saldo, ipemilik transaksi cukup membuktikan pengetahuan mengenai nilai eksponen $y_1, y_2, \ldots, y_{new}$ dan Y pada persamaan 1 ehubungan dengan generator $Q_1, Q_2, \ldots, Q_{new}$ dan h_2. Given Mengingat bahwa generator-generator ini bersifat publik, pengirim dapat memberikan bukti representasi dari nilai $\frac{\mathbf{A}}{\mathbf{B}}$ sehubungan dengan generator $Q_1, \ldots, Q_{new}, h_2,$ yang kemudian dapat diverifikasi secara publik oleh semua peserta jaringan.

5 Performa

Perubahan protokol ini menghasilkan pengorbanan dalam hal penyimpanan dan efisiensi komputasi dibandingkan dengan [3].

1. Konstruksi ini mengharuskan setiap koin baru yang dicetak secara eksplisit terkait dengan alamat penerima Q beserta bukti representasinya sehubungan dengan generator g dan h1 . Oleh karena itu, setiap koin yang dicetak akan terdiri dari komitmen C, alamat Q, dan bukti representasi yang sesuai P. Hal ini membutuhkan sebuah elemen grup tambahan dan dua skalar tambahan setiap kali pencetakan.
2. Sistem pembayaran menyiratkan bahwa data pribadi koin dikomunikasikan dengan penerima baik melalui saluran samping yang aman atau langsung pada blockchain. Dalam kasus terakhir, pengirim mengenkripsi semua data pribadi koin dengan kunci publik penerima dan memasukkannya ke dalam transaksi. Dalam konstruksi baru kami, data pribadi ini adalah elemen y dan V; dalam [3] adalah y, V, dan R. Pengurangan ruang tergantung pada metode yang digunakan untuk mengenkripsi nilai-nilai ini kepada penerima.
3. Bukti saldo (yang terdiri dari satu bukti representasi) akan membutuhkan tambahan N_{new} - 1 elemen grup. Untuk transaksi dengan satu keluaran, tidak ada biaya tambahan.
4. Bukti rentang dalam konstruksi ini diproduksi menggunakan komitmen Pedersen standar, alih-alih komitmen buta ganda pada protokol aslinya. Ketika menggunakan Bulletproofs [2], ini merupakan pengurangan penyimpanan elemen grup tunggal.

Kami mencatat bahwa verifikasi batch dari bukti pengeluaran masih dimungkinkan dengan konstruksi kami yang telah diperbarui.

6. Pekerjaan Lebih Lanjut

Konstruksi yang disajikan di sini mengurangi masalah penelusuran yang ada pada protokol transaksi Lelantus yang asli. Akan tetapi, hal ini mengharuskan penerima untuk memberikan data alamat yang baru kepada pengirim untuk setiap transaksi. Penerima diharapkan untuk mempublikasikan satu alamat tunggal sehingga pengirim dapat memperoleh alamat satu kali yang bersifat sementara sesuai kebutuhan. Akan tetapi, mendesain dengan aman sebuah konstruksi yang tahan terhadap pelacakan masih menjadi tugas yang terbuka.

Terakhir, konstruksi ini bersifat informal dan tidak memiliki analisis keamanan.

Referensi

1. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, pages 62–73, New York, NY, USA, 1993. ACM.
2. B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 315–334, May 2018.
3. Aram Jivanyan. Lelantus: Towards confidentiality and anonymity of blockchain transactions from standard assumptions. Cryptology ePrint Archive, Report 2019/373, 2019. `https://eprint.iacr.org/2019/373`.

4. I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous distributed e-cash from Bitcoin. In *2013 IEEE Symposium on Security and Privacy*, pages 397–411, May 2013.
5. T. Ruffing, S. A. Thyagarajan, V. Ronge, and D. Schroder. Burning Zerocoins for fun and for profit - a cryptographic denial-of-spending attack on the Zerocoin protocol. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 116–119, June 2018.