Implementación de Canales Paralelos en un Protocolo Non Interactive Dining Cryptographers

Pablo García[1], Jeroen van de Graaf[2], Germán Montejano[3], Silvia Bast[1], Oscar Testa[1]

[1] Departamento de Matemática - Universidad Nacional de La Pampa
Av. Uruguay 151- (6300) Santa Rosa - La Pampa - Argentina
{pablogarcia, silviabast, otesta}@exactas.unlpam.edu.ar
http:/www.exactas.unlpam.edu.ar

[2] Departamento de Ciência da Computação - Universidade Federal de Minas Gerais -
Av. Antonio Carlos, 6627 – 31270-010 - Belo Horizonte – Minas Gerais - Brasil
jvdg@dcc.ufmg.br
http://www.dcc.ufmg.br/jvdg

[3] Departamento de Informática - Universidad Nacional de San Luis
Ejército de los Andes 950 – (5700) San Luis – San Luis – Argentina
gmonte@unsl.edu.ar
http://www.unsl.edu.ar

Resumen *Dining Cryptographers* es un protocolo criptográfico que provee un nivel incondicional de seguridad para la privacidad de los mensajes publicados por un grupo de usuarios de una red, exigiendo la concurrencia online de los participantes. Sin embargo, existen múltiples situaciones prácticas en las que esta condición no necesariamente se verifica, como por ejemplo, voto electrónico.

En consecuencia, y atendiendo a la riqueza de la propuesta, surge una derivación denominada *Non Interactive Dining Cryptographers* (NIDC) que intenta explotar todo el potencial del esquema original, procurando cubrir un rango mayor de problemas a los que el modelo pueda aplicarse. Con ese objetivo, el nuevo esquema relaja la condición de concurrencia temporal de los participantes.

En NIDC, el almacenamiento de los votos se basa en la utilización de un vector único de slots. El presente trabajo tiene dos objetivos: exponer las ventajas de reemplazar ese enfoque por otro que implemente múltiples canales paralelos y proponer una metodología que permita encontrar los valores óptimos para los parámetros involucrados en la administración del espacio destinado a registrar los sufragios en un protocolo NIDC, mediante la aplicación del nuevo enfoque.

Keywords: Colisión, slot, seguridad incondicional, anonimato, voto electrónico, Dining Cryptographers, Birthday Paradox, Occupancy Problem, canales paralelos.

1. Introducción y motivación

En el ámbito de los esquemas de voto electrónico, no existe acuerdo sobre el nivel de seguridad que debe asignarse a la privacidad de los votantes. Los esquemas basados en Mix Net (ver [1]), por ejemplo, protegen incondicionalmente el desarrollo de la votación, pero proveen seguridad computacional para el anonimato. Como se afirma en [2], parece evidente que tal orden debe invertirse, dado que el proceso de votación se desarrolla en un tiempo finito y que, una vez finalizado, los resultados se publican. El anonimato, en cambio, debería ser protegido indefinidamente.

En consecuencia, resultan de interés aquellos protocolos que protejan incondicionalmente la privacidad, resultando aceptable un nivel computacional para el proceso eleccionario. *Dining Cryptographers*, presentado en [3], pertenece a ese grupo. En particular, una derivación propuesta en [2] (*Non Interactive Dining Cryptographers*, NIDC), resulta aplicable a voto electrónico por no exigir la concurrencia en el tiempo de todos los participantes. En [4] se presenta una metodología del mismo estilo, más orientada a la descripción de técnicas antifraude.

Específicamente, el presente trabajo se enfoca en minimizar la probabilidad de pérdida de sufragios en un esquema NIDC. Concretamente, se busca:

- Demostrar que si se utilizan parámetros correctos, la implementación de canales paralelos disminuye severamente la probabilidad de pérdida de sufragios.
- Proponer una metodología que permita definir los valores de todos los parámetros si se plantea la exigencia de mantener la probabilidad de pérdida de votos por debajo de un valor dado.

El voto electrónico sólo puede resultar exitoso si muestra ventajas reales sobre un esquema manual tradicional. En ningún caso resultará de interés reemplazar un modelo por otro con menor funcionalidad. El presente trabajo propone mejoras concretas en un punto fundamental del esquema NIDC: la necesidad de minimizar la pérdida de sufragios.

2. Breve descripción de NIDC

NIDC se deriva de *Dining Cryptographers*, que es un protocolo que presenta niveles de seguridad incondicional para el anonimato asociado a la emisión de una información determinada, a través de canales públicos, que puede describirse de la siguiente manera:

Tres criptógrafos comparten una cena en un restaurant. Al llegar el momento de pagar, el mozo les indica que la adición ya ha sido abonada y, que quién lo hizo, no desea que se conozca su identidad. Los criptógrafos desean saber si

alguno de los comensales fue quien realizó el pago, o si la cuenta fue abonada por alguien que no pertenece al grupo. Ellos pretenden saber solamente eso: si pagó alguno de ellos o no. En caso de un pagador externo, el anonimato está garantizado, pero si fuese un integrante del grupo, los demás respetan el derecho a invitar y no desean saber la identidad del pagador.

Planteado de esta manera, la solución que encuentran es la siguiente:

Cada uno de los comensales lanza una moneda al aire. Observa el resultado obtenido y lo comparte con su vecino de la izquierda. Luego, cada uno de ellos ve exactamente dos monedas, la propia y la del vecino que comparte con él. Finalmente, cada uno debe indicar si las dos monedas que pudo observar son "iguales" o "diferentes", con la condición de que si alguno de ellos abonó la adición, debe mentir con respecto a su afirmación.

En las condiciones descriptas, si el número de criptógrafos que proclama *"diferentes"* es impar, el pagador se encuentra en el grupo de comensales. Un número par, en cambio, indica que el pagador es externo al grupo.

La demostración formal de que el esquema es seguro se expone por primera vez en [5] y se formaliza con mayor precisión en [6], utilizando el concepto de *Vista (View):*

Una vista es una variable aleatoria basada en el conjunto de información con la que cuenta un participante determinado al finalizar el proceso.

Concretamente, la vista de un participante estará conformada por:

- Las entradas que él mismo aporta al proceso.
- Sus conjuntos de bits aleatorios.
- Todos los mensajes que haya enviado o recibido.

Si podemos probar que la vista de la que dispone un usuario determinado no permite determinar las elecciones realizadas por los demás participantes en ningún caso, el anonimato queda garantizado. En particular, para analizar el protocolo *Dining Cryptographers*, podemos distinguir los siguientes elementos y analizar cuáles de ellos están visibles para cada participante:

Las monedas: de acuerdo a la mecánica del modelo, cada participante ve su propia moneda y la de su vecino de la izquierda. Denominaremos:

$$r_i \in \{Cara, Ceca\}$$

al valor obtenido en la acción de lanzar la moneda i.

La información de inversión: Este elemento será $m_i \in \{True, False\}$. Si m_i es $True$, implica que el participante pagó la cuenta y, por lo tanto, miente al expresar el resultado que observa de la comparación de las dos monedas que puede observar. Un valor $False$ implica lo contrario.

La información de comparación de dos monedas: Para este dato se utilizará $x_i \in \{Iguales,\ Diferentes\}$. Obviamente un valor *Iguales* implica que el participante i declara que los valores de ambas monedas que puede ver son coincidentes.

Por lo tanto, puede definirse en esos términos la seguridad del protocolo. Será suficiente con analizar las vistas que un participante determinado dispone ante todos los casos posibles, dado que la simetría garantiza que las conclusiones pueden generalizarse.

Se observa entonces las vistas que el participante P_1 podría tener a disposición. Los casos son los siguientes:

El pagador es externo. En este caso, el anonimato está garantizado.

P_1 **es el pagador.** Está situación también es trivial.

P_2 **es el pagador.** La vista que P_1 tiene a disposición es la siguiente:

$$V_1 = (r_1, -, r_3, m_1, -, -, x_1, x_2, x_3)$$

P_3 **es el pagador.** Ante esta situación, P_1 ve:

$$V_1 = (r_1, -, r_3, m_1, -, -, x_1, x_2, x_3)$$

Queda claro que las vistas de los dos últimos casos tienen la misma distribución. Concretamente, los valores de r_1 ,r_3, m_1 y x_1 serán exactamente iguales en ambos casos. x_2 y x_3 , en cambio, presentarán valores opuestos dependiendo de quien haya pagado la cuenta. Sin embargo, eso no le entrega información adicional a P_1 , porque tales valores dependen de r_2 , valor que él no conoce y que presenta equiprobabilidad de tomar cualquiera de los dos valores posibles.

Por lo tanto, si alguno de sus compañeros abonó la cena, P_1 no puede distinguir quién fue, dado que:

$$P(P_2(\ pagó)) = P(P_3(\ pagó)) = \frac{1}{2} \tag{1}$$

En consecuencia, *Dining Cryptographers* reviste gran interés en aplicaciones criptográficas. Sin embargo, presenta la limitación de exigir la concurrencia en el tiempo de todos los participantes. Existen muchas aplicaciones que exigen anonimato incondicional, pero que muestran características asincrónicas. En consecuencia, surge una metodología que mantiene los niveles de seguridad del esquema original pero no exige la concurrencia temporal de todos los participantes. Para ello, combina el concepto de *Firmas Ciegas* descripto detalladamente en [7] con una derivación del protocolo de Chaum que se presenta en [2]: *Non Interactive Dining Cryptographers (NIDC)*, que no exige la concurrencia online de todos los participantes. Por tratarse de un protocolo sin retroalimentación, presenta algunas características novedosas. Se puede describir en tres pasos:

1. En una fase preliminar, cada par de participantes intercambia bits aleatorios.
2. Basándose en los bits aleatorios y la entrada de las partes, se publica un mensaje.
3. Todos los mensajes se combinan, de tal manera que se cancelan todos los bits aleatorios y lo único que permanece son las entradas de todos los participantes.

El anonimato es garantizado directamente por *Dining Cryptographers* de acuerdo al análisis de las *vistas (views)* realizado previamente. En consecuencia, si se prepara un protocolo que permita distinguir mensajes, los mismos serán interpretados evitando la posibilidad de conocer la autoría de cada uno de ellos.

La protección de la información circulante sólo debe soportar el lapso de tiempo que corresponda al proceso de votación. Todas las firmas se darán a conocer una vez cerrada la elección. Hacer pública esa información deriva en un aumento significativo de la transparencia del procedimiento.

Aparecen entonces los flujos de información del tipo *desafío y respuesta*, que permiten verificar que el mensaje que se desea publicar no contradice ninguna afirmación previa. Esto se implementa mediante la utilización de un esquema *commitment:*

En criptografía, se denomina "commitment" a cualquier técnica que pueda aplicarse para "comprometer" una información de manera que, al finalizar el proceso, pueda verificarse que la misma no fue modificada.

Existen muchas modalidades de implementación. En particular, NIDC se basa en la heurística de Feige-Shamir ([8]): con posterioridad al *commitment*, se implementa un esquema que permite a los participantes controlar que el mensaje es coherente con los valores comprometidos inicialmente. Si la implementación es apropiada, el modelo se comporta de manera segura sin la necesidad de concurrencia temporal.

Concretamente, NIDC implementa una estrategia basada en BCX *(Bit Commitments con XOR)*. La solución adoptada consiste en un protocolo integrado por *commitments* basados en funciones de hash. La idea es representar cada BCX como un vector de pares de *"bit commitments"* simple, tal que si a cada par se le aplica un XOR, el resultado obtenido es el valor del bit comprometido. La técnica, entonces, habilita la posibilidad de desafíos sobre una mitad del bit commitment, pero sin revelar su valor.

La manera exacta en que se implementa la administración de BCX se describe detalladamente en [2], [5], [6] y [11]. En [6] y [12] se presenta un protocolo alternativo que mantiene los niveles de seguridad originales pero que resulta mucho más eficiente en términos de las operaciones involucradas. Esa propuesta se basa en propiedades de los logaritmos discretos.

En este trabajo en particular, en cambio, el interés se enfoca en la seguridad de los sufragios. En consecuencia, se analiza en la próxima sección todo lo relacionado con la probabilidad de perder votos en un esquema NIDC.

3. Manejo de Colisiones en un esquema NIDC

En un protocolo NIDC, los votos se almacenan en un vector de slots. El anonimato queda garantizado por la elección totalmente aleatoria de la ubicación de un sufragio. En consecuencia, es posible que dos o más votantes elijan el mismo slot. Tal situación se denomina *colisión* y da lugar a la pérdida de todos los votos coincidentes. Si se implementa un vector simple para el almacenamiento, la referencia teórica más conocida es Birthday Paradox, desarrollada detalladamente en [9]:

En un grupo de 23 personas la probabilidad de que dos cumplan años el mismo día es cercana a $\frac{1}{2}$.

Tal situación es desfavorable, dado que, la proporción de slots vacíos es alta y la probabilidad de que no se produzcan colisiones muestra valores muy alejados de algo que pueda resultar aceptable en un esquema de voto electrónico.

Por otro lado, $N = 23$ es un valor mucho más pequeño que aquellos que puedan resultar de interés para voto electrónico. Por ejemplo, un recinto en Brasil es de alrededor de 500 votantes.

Se busca, entonces, un enfoque alternativo que permita optimizar el almacenamiento destinado a los sufragios. Lo primero que se observa es que aún en el mejor caso (las 23 personas cumplen años en fechas diferentes), la cantidad de slots que no serán utilizados es 342, entonces tenemos aproximadamente un 6,3 % de slots ocupados y un 93,7 % de slots vacíos. En consecuencia, por cada slot que contiene un sufragio, hay más de 15 que no reciben votos.

Aparece entonces la idea de buscar una manera de aprovechar de manera más eficiente tal almacenamiento. La propuesta consiste en dividir la totalidad de slots en $Q>1$ canales paralelos y depositar una ocurrencia de cada sufragio en cada uno de los canales. El disparador de tal hipótesis es una propiedad de los sucesos independientes:

$$P(A \cap B) = P(A)P(B) \tag{2}$$

Es evidente que un voto se perderá solamente si colisiona en todos los canales. Si bien el número de colisiones va a aumentar, dado que cada canal tendrá una medida menor que el vector único, los resultados finales en términos de votos perdidos resultan mejores, tal como se desprende de los desarrollos matemáticos y simulaciones expuestas en [5], [6] y [11].

4. Implementación de Canales Paralelos

Sean:

$N = \#$ votos.

$T = \#$ total de slots.

$S = \#$ slots en cada canal.

$\varepsilon = \frac{N}{S}$.

$Q : \#$ canales paralelos a implementar.

$Q_{ot} : \#$ canales paralelos. Valor óptimo teórico.

$Q_{oa} : \#$ canales paralelos. Valor óptimo aplicable.

PVP : porcentaje de votos perdidos en un acto eleccionario.

En [5] se presentaron tres fórmulas que resultan de utilidad. Las mismas se inspiran en los desarrollos de [10], en lo referido al abordaje de *Ocuppancy Problem*. La primera describe el valor esperado para la variable PVP, porcentaje de votos perdidos.

$$E(PVP) = (1 - e^{-\frac{N}{S}})^Q \tag{3}$$

La segunda describe el valor óptimo de Q (cantidad de canales paralelos):

$$Q_{ot} = (ln2)\frac{T}{N} \tag{4}$$

Obviamente, el valor que se aplique debe ser entero. Por tal razón se redondea hacia arriba:

$$Q_{oa} =\mid Q_{ot} \mid +1 \tag{5}$$

La tercera ecuación se relaciona con la variable S. Concretamente, existe un valor óptimo para la cantidad de slots que debe implementarse para un número de votantes N dado:

$$S =\mid \frac{N}{ln2} \mid +1 \tag{6}$$

Cabe mencionar que, de manera complementaria a los desarrollos teóricos, como parte del proyecto se implementó un simulador de actos eleccionarios con los siguientes objetivos:

1. Confirmar de manera práctica los resultados matemáticos. Las fórmulas expuestas en la sección anterior tienen su correlato en los valores obtenidos por simulación.
2. Permitir una observación más clara de las variables involucradas, a los efectos de confirmar o descartar ideas surgidas de manera intuitiva.

Los resultados proporcionados por el simulador están descriptos detalladamente en [11] y [5], resultando los mismos totalmente coherentes con lo expresado desde la formalidad matemática. La deducción de todas las fórmulas matemáticas presentadas se expone en [6].

5. Propuesta para una Solución Integral

Un problema práctico que resulta importante resolver se plantea mediante la siguiente pregunta:

¿Qué valores deben tomar los parámetros para que la probabilidad de que la cantidad de votos perdidos sea nula resulte mayor o igual que un valor dado?

Si se piensa en aplicar las metodologías propuestas en un sistema de voto electrónico concreto, es imprescindible poder cuantificar la probabilidad de que no se pierdan votos en un acto eleccionario determinado. Para enunciar una cota, se propone un enfoque que se basa en el análisis de las colisiones.

Definimos:

V_i**:** i-ésimo sufragio.

R_{ij}**:** Suceso que indica que V_i ocupa el j-ésimo slot.

C_{ijk}**:** V_i colisiona con V_j en el k-ésimo canal.

A_i**:** V_i colisiona en todos los canales.

L**:** # sufragios que se pierden en todos los canales simultáneamente.

I**:** # slots en que se producen colisiones múltiples

Para $Q = 1$, Si V_1 cae en el slot 1, la probabilidad de que colisione con V_2, consiste en que ambos caigan en el slot 1:

$$Pr(C_{121} \mid R_{11}) = \frac{1}{s}\frac{1}{s} = \frac{1}{s^2} \tag{7}$$

Luego, la probabilidad de que los sufragios V_1 y V_2 colisionen en cualquier slot es:

$$Pr(C_{121}) = \frac{1}{s^2}S = \frac{1}{s} \tag{8}$$

Pero la probabilidad de colisión será similar para todos los demás sufragios:

$$Pr(C_{121}) = Pr(C_{1j1})\,\forall j \in \{3..N\} \tag{9}$$

En consecuencia, la probabilidad de que V_1 se pierda en el canal único está dado por la expresión:

$$Pr(B_{11}) = \frac{1}{S}(N-1) - Pr(I) \tag{10}$$

De la ecuación anterior se deriva una más conveniente:

$$Pr(\overline{B_{11}}) = 1 - \frac{1}{S}(N-1) + Pr(I) \tag{11}$$

El valor de $P(I)$ es bajo, pero positivo. Por lo tanto:

$$Pr(\overline{B_{11}}) > 1 - \frac{1}{S}(N-1) \tag{12}$$

La fórmula anterior permite explicarle a un votante la probabilidad de que su voto se pierda o no, en un esquema monocanal. La precisión de la fórmula aumenta en la medida en que $S \to \infty \wedge N \to \infty$. Cuando se incorporan más canales, se puede afirmar:

$$Pr(A_i) = Pr(B_{i1})^Q < (\frac{1}{S}(N-1))^Q\,\forall i \in \{1..N\} \tag{13}$$

Entonces, por ejemplo, para :

- $S = 10$ slots.
- $N = 4$ votantes.
- $Q = 4$ canales paralelos.

La probabilidad de que un voto específico se pierda es:

$$Pr(A_i) < (\frac{1}{S}(N-1))^Q$$
$$Pr(A_i) < (\frac{1}{10}(4-1))^4$$
$$Pr(A_i) < (\frac{1}{10}(3))^Q$$
$$Pr(A_i) < (\frac{3}{10})^4$$
$$Pr(A_i) < 0,0081$$

Finalmente, la probabilidad de que ningún voto se pierda simultáneamente en todos los canales puede acotarse de la siguiente manera:

$$Pr(X) = Pr(\overline{A_1}) \cap Pr(\overline{A_2}) \cap ... \cap Pr(\overline{A_n}) \tag{14}$$

Pero:

$$Pr(\overline{A_1}) = Pr(\overline{A_2}) = ... = Pr(\overline{A_N}) \tag{15}$$

Además, son sucesos independientes. Luego:

$$Pr(X) = Pr(\overline{A_1})^n \tag{16}$$

O, lo que es lo mismo:

$$Pr(X) = 1 - Pr(A_1)^n \tag{17}$$

Finalmente, por la ecuación (13) se puede afirmar:

$$Pr(X) > (1 - (\frac{1}{s}(n-1))^q)^n \tag{18}$$

Lo cual constituye una cota superior muy apropiada para describir la probabilidad de pérdida de votos en una acto eleccionario concreto con los parámetros descriptos.

Para mostrar el comportamiento de la fórmula, la Figura 1, compara la curva correspondiente a la fórmula de Birthday Paradox, con la cota propuesta, para un único canal y desde 1 a 170 slots.

En base a las fórmulas enunciadas previamente se presenta una propuesta concreta para obtener valores de S y Qoa (y en consecuencia, $T = Qoa\ S$) para que la probabilidad del evento:

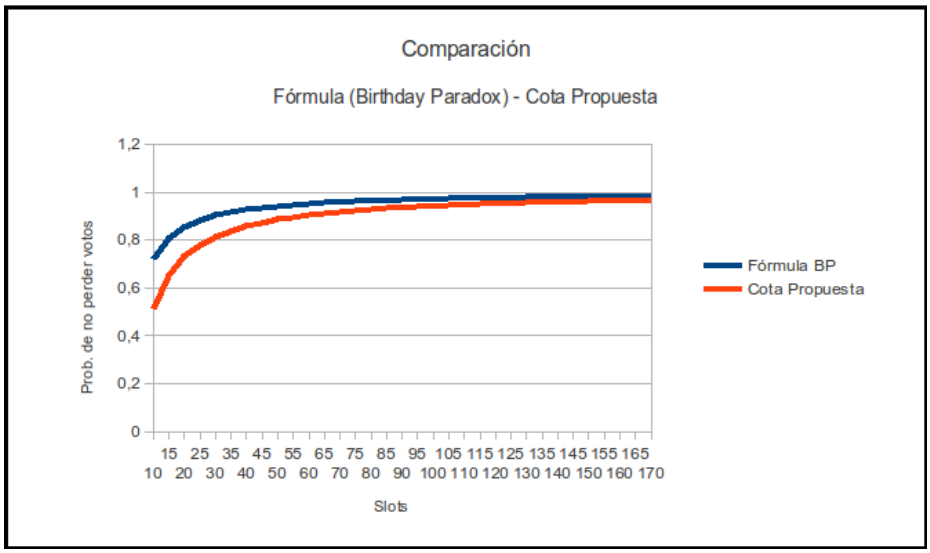

Figura 1: Birthday Paradox vs. Cota Propuesta

X="No se pierde ningún voto".

tenga una probabilidad mayor que un valor dado. Se deben llevar a cabo los siguientes pasos:

1. Se elige un valor de S, dado por la fórmula (6), es decir:

$$S = \left| \frac{N}{ln2} \right| + 1$$

   La metodología de la selección permite ir incrementando el valor de Q, con la garantía de que el mismo siempre responderá a la ecuación que enuncia el valor de Q óptimo. Además, se toma la parte entera del cociente y se le suma 1.

2. A continuación, se arma en una planilla de cálculo como la que se muestra en el Cuadro 1:

	A	**B**	**C**	**D**	**E**	**F**	**G**
1	N	S	Q	CS	CO	**¿Es Mayor?**	T
2	480	Fórmula 1	1	0,999	Fórmula 2	Fórmula 3	$=C2*D2$

Cuadro 1: Definición de los valores óptimos de S y Q

Donde:

N, S, Q, **y** T**:** Mantienen los roles definidos en secciones anteriores.

CS**:** Cota solicitada.

CO**:** Cota obtenida.

Fórmula 1: =ENTERO (A2/LN(2))+1

Fórmula 2: =POTENCIA(1-(POTENCIA((1/C2)*(A2-1);D2));A2)

Fórmula 3: =SI(F2>E2;"SI";"NO")

Luego, para encontrar los valores que garanticen la seguridad buscada, basta con incrementar el contenido de la celda D2, que contiene el valor de Q, hasta que la celda G2 almacene el valor "SI", lo que indicará que el objetivo fue alcanzado. Para ejemplificar, se muestran en el Cuadro 2 los valores obtenidos para 480 votantes con diferentes niveles de seguridad.

N	S	Q	CS	CO	**¿Es Mayor?**	T
480	693	23	0,9	0,9064621422	SI	15939
480	693	30	0,99	0,9926259386	SI	20790
480	693	36	0,999	0,9991932325	SI	24948
480	693	42	0,9999	0,9999119929	SI	29106
480	693	48	0,99999	0,9999904027	SI	33264
480	693	55	0,999999	0,9999992766	SI	38115

Cuadro 2: Valores Obtenidos para S y Q

Se elige el modelo basado en planilla de cálculo porque resulta más explicativo. Es trivial implementar una aplicación que calcule los valores óptimos para N y CS dados.

6. Trabajos Relacionados

El presente trabajo tiene sus orígenes en [2], donde se deja para investigaciones futuras la obtención de optimizaciones en dos puntos muy concretos: manejo de colisiones y administración de maniobras fraudulentas. Los desarrollos parciales se ven en diferentes publicaciones:

- En [11] se muestran los primeros resultados de experimentos realizados para analizar la optimización obtenida al aplicar canales paralelos.
- En [5] se presentan por primera vez las fórmulas (3), (4) y (5) que se mencionan en el presente trabajo.

- En [12] se expone un protocolo destinado a reemplazar al original de NIDC, que mantiene los niveles de seguridad, pero proporcionando una eficiencia mucho mayor en términos de operaciones de máquina. El nuevo esquema se basa en commitments de Pedersen, en base a propiedades publicadas en [13].
- Todos los elementos anteriores se recopilan luego en [6], donde se agrega una metodología concreta que determina los valores óptimos para las magnitudes involucradas en la implementación de canales paralelos destinados al almacenamiento de sufragios en un esquema NIDC.

7. Conclusiones y Problemas Abiertos

La conclusión central de este trabajo es que es posible optimizar el espacio destinado al almacenamiento de sufragios mediante la utilización de canales paralelos si se verifican dos condiciones:

- Se replica cada voto una sola vez en cada canal paralelo.
- Se eligen apropiadamente los parámetros involucrados, aplicando la técnica expuesta en la sección 5.

A partir de esa afirmación se desprenden una serie de elementos que deben mencionarse:

1. El valor esperado de la variable PVP (porcentaje de votos perdidos), puede ser estimada aplicando la fórmula (3):

$$\mathrm{E}(PVP) = (1 - e^{\frac{-N}{S}})^Q$$

2. El número de slots de cada canal individual debe mantenerse en un nivel razonablemente superior a la cantidad de votos. Si no se verifica esa condición, la cantidad de colisiones aumenta de manera considerable y la calidad de los resultados decae. Para garantizar que tal situación no se produzca, se puede utilizar la ecuación (6), que define, para un número fijo de votantes N, el valor óptimo de la variable S (cantidad de slots para cada canal paralelo):

$$S = \mid \frac{N}{ln2} \mid +1$$

3. Para valores dados de T y N, existe un número óptimo de canales paralelos. Tal valor se expresa por la ecuación (4):

$$Q_{ot} = (ln2)\frac{T}{N}$$

Tal fórmula debe llevarse al entero siguiente, tal como fue enunciado en la fórmula (5)

$$Q_{oa} =\mid Q_{ot} \mid +1$$

Como se explicó oportunamente, se redondea al entero siguiente debido a que el valor que se aplique de Q debe ser necesariamente entero.

4. Es muy importante la obtención de una cota superior apropiada para la probabilidad de que no se pierdan votos. La misma se obtiene mediante la aplicación de la ecuación (18):

$$Pr(X) > (1 - (\tfrac{1}{s}(n-1))^q)^n$$

5. Finalmente, en base a las fórmulas enunciadas, se presenta una técnica concreta que sistematiza la búsqueda de los valores óptimos para S y Q de manera que la probabilidad de que no se pierda ningún voto resulte mayor o igual que un valor dado.
6. Por lo expuesto en [6], se considera probado que la repetición de datos en un mismo canal no genera beneficios. Las simulaciones llevadas a cabo en ese sentido demuestran que resulta más relevante el aumento de las colisiones que la mejora que reportaría la publicación de múltiples instancias de un mismo dato en un canal. Efectivamente, al duplicar las réplicas se genera una variante de *Birthday Paradox* con el doble de participantes.

Por último, un objetivo futuro de esta línea de investigación es analizar si es posible utilizar herramientas para recuperación de colisiones y el alcance de las mismas. Por ejemplo, si en cada réplica se almacena información que indique donde se almacenaron las demás copias, un sufragio que haya colisionado en todos los canales podría recuperarse mediante una operación XOR, si se verifica que en alguna de esas colisiones coincide con un sufragio que tiene alguna instancia válida. Se desea definir el alcance exacto de tales herramientas y determinar si es posible encontrar alternativas para colisiones múltiples.

Referencias

1. **Jakobsson M., Juels, A., Rivest, R.**: "Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking"- AUSENIX Security 02. Vol. 7. Ps. 339-353. 2002.
2. **Van de Graaf J.**: "Anonymous One Time Broadcast Using Non Interactive Dining Cryptographer Nets with Applications to Voting". Publicado en: "Towards Trustworthy Elections". Ps. 231-241. Springer-Verlag Berlin, Heidelberg. ISBN:978-3-642-12979-7. 2010.
3. **Chaum D.**: "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability". Journal of Criptology. 1988.
4. **Bos J.**: "Practical Privacy"- Technische Universiteit Eindhoven, ISBN: 90-6196-405-9. 1992.
5. **Van de Graaf J., Montejano G., García P.**: "Manejo de Colisiones en un Protocolo Non Interactive Dining Cryptographers". Anales de las 42 Jornadas Argentinas de Informática e Investigación Operativa (JAIIO, ISSN: 1850-2776). Workshop de Seguridad Informática (WSegI 2013, ISSN: 2313-9110). Ps. 29 a 43. Septiembre 2013.
6. **García P.**:"Optimización de un esquema Dining Cryptographers Asíncrono". Tesis para acceder al grado de Magister en Ingeniería de Software de la UNSL. Directores: Jeroen van de Graaf, PhD (UFMG), Belo Horizonte, Brasil y Dr. Germán Montejano (UNSL). San Luis, Argentina. Fecha de defensa: 12/11/2013. Calificación: Sobresaliente.
7. **Fujioka A., Okamoto T., Ohta K.**: "A Practical Secret Voting Scheme for Large Scale Elections". AUSCRYPT 1992. LNCS, Vol. 718. Páginas 244 a 251. Springer Heidelberg. 1993.
8. **Kizza J.**: "Feige-Fiat-Shamir ZKP Scheme Revisited". Journal of Computing and ICT Research, Vol. 4, No. 1,pp. 9-19. http://www.ijcir.org/volume4-number1/article2.pdf.
9. **Flajolet P., Gardy D., Thimonier L.**: 'Birthday paradox, coupon collectors, caching algorithms and self-organizing search'. Discrete Applied Mathematics 39, ps. 207-223. North-Holland. 1992
10. **Feller W.**: "An Introduction to Probability Theory and its Applications". Volúmen I. Tercera Edición. John Wiley and Sons. New York, 1957.
11. **Van de Graaf J., Montejano G., García P.**: "Optimización de un esquema "Ocuppancy Problem" orientado a E – Voting". Memorias del XV Workshop de Investigadores en Ciencias de la Computación 2013 (WICC 2013). Ps. 749 - 753. ISBN: 9789872817961.
12. **Van de Graaf J., Montejano G., García P.**: 37. "Optimización de un Protocolo Non-Interactive Dining Cryptographers ". Congreso Nacional de Ingeniería Informática / Sistemas de Información . CoNaIISI 2013. 21 y 22 de noviembre de 2013. Córdoba, Argentina.
13. **Van de Graaf J.**: "Voting with Unconditionally Privacy: CFSY for Booth Voting". IACR Cryptology ePrint Archive. Ps. 574-579. 2009.