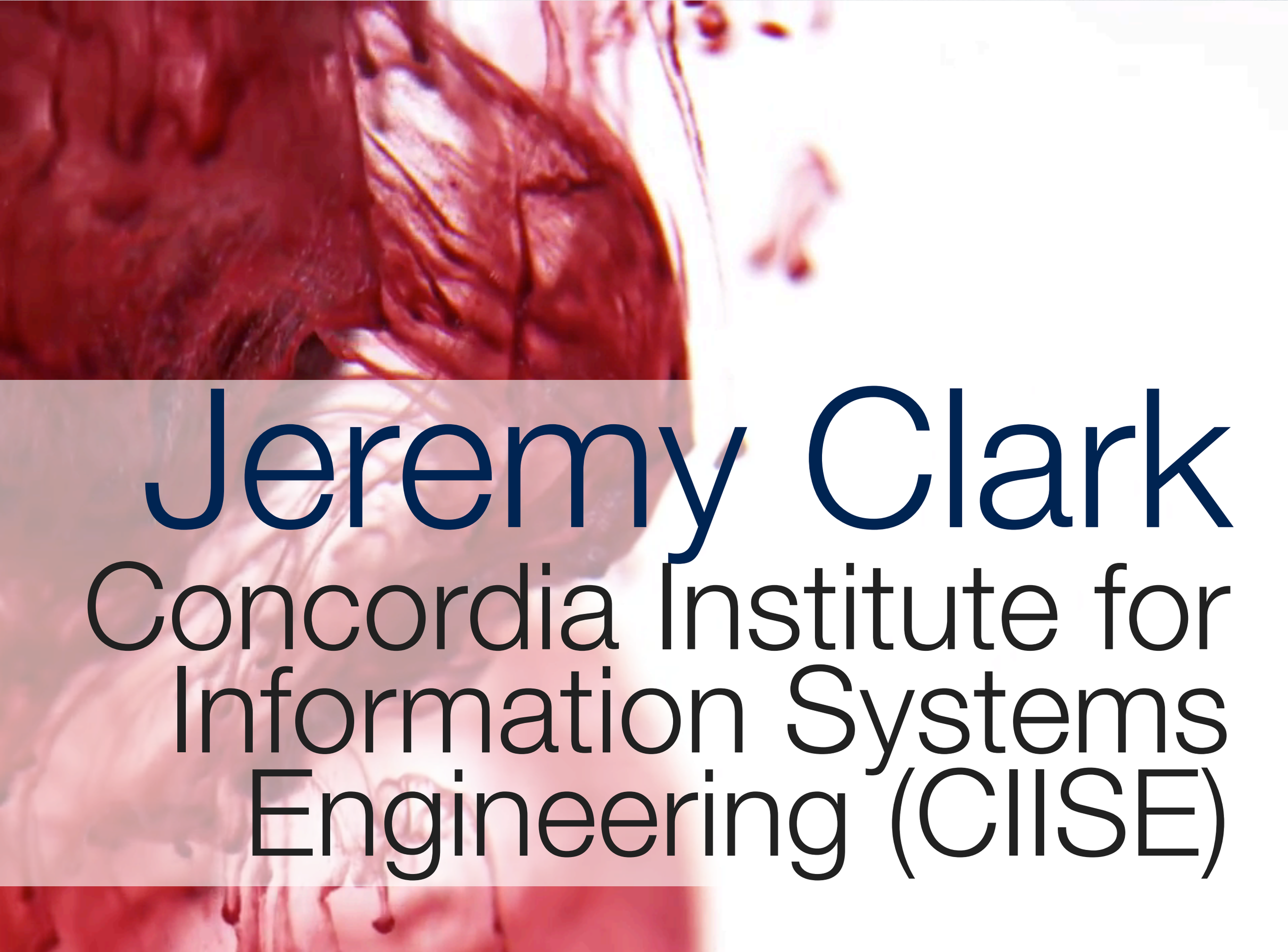


Jeremy Clark

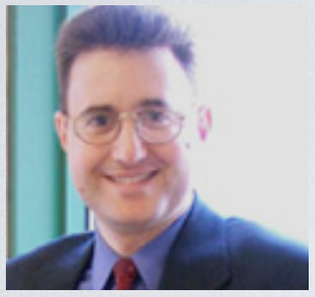
Concordia Institute for Information Systems Engineering (CIISE)

Concordia University

Concordia Institute for Information Systems Engineering

Faculty of Engineering and Computer Science

- Foundation of Cryptography
- Crypto-Protocol and Network Security
- Operating Systems Security
- Malware Defenses and Application Security
- Security Evaluation Methodologies
- Database Security and Privacy
- Security and Privacy Implications of Data Mining
- Wireless Network Security
- Cybercrime Investigations
- Cloud Computing Security and Privacy
- Recent Developments in Information Systems Security
- Smart Grids and Control System Security
- Trusted Computing



Mourad Debbabi, Cyber forensics

Mohammad Mannan, Systems security

Lingyu Wang, Data privacy

Amr Youssef, Cryptography

SSL/TLS

Election Security

Bitcoin

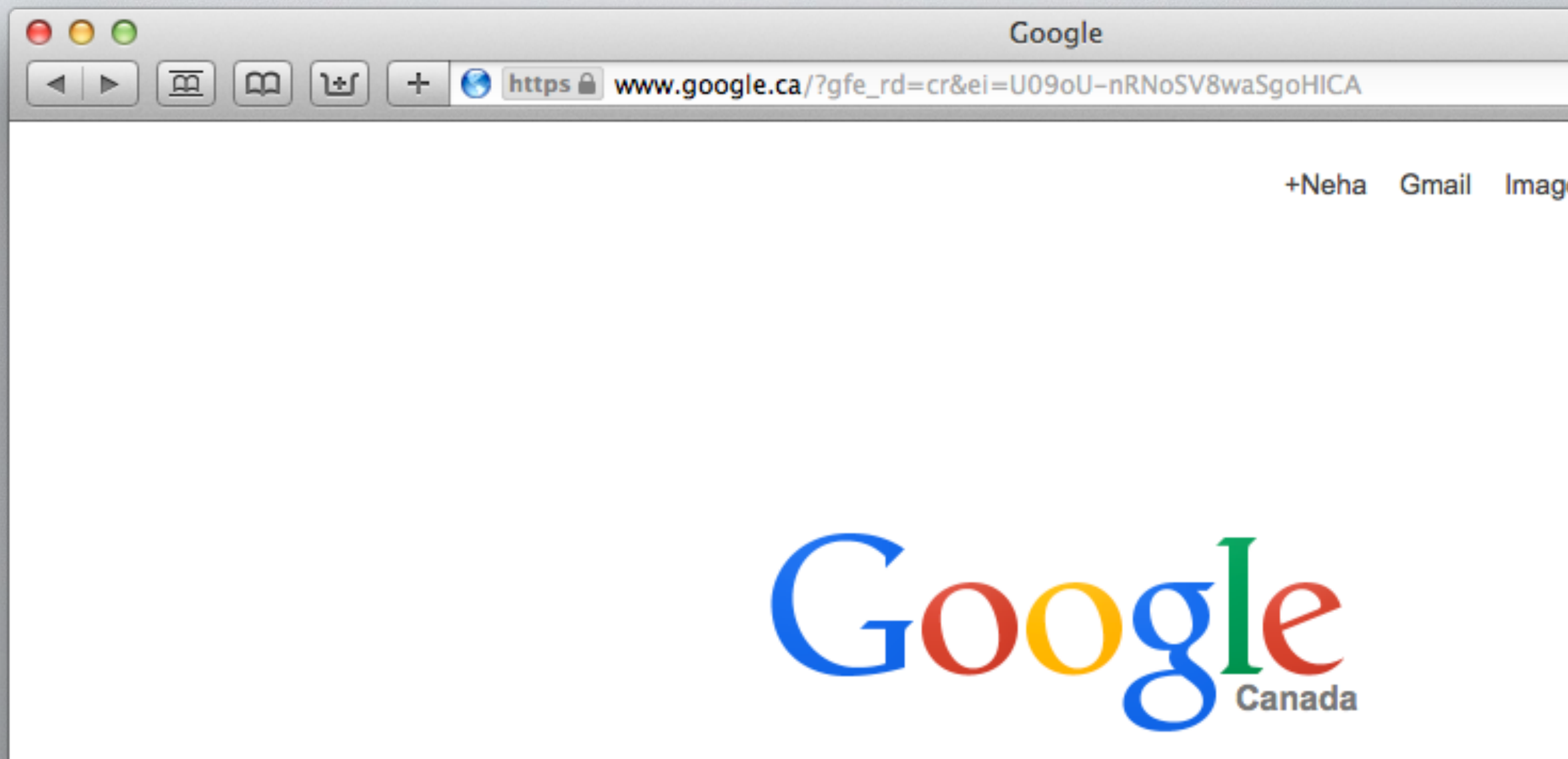
Genomic Privacy

Android Security

Financial Market Security

SSL/TLS

HTTPS (HTTP over SSL/TLS)



SSL/TLS

HTTPS (HTTP over SSL/TLS)

Despite being decades old and standardized, still a host of issues

SSL/TLS

HTTPS (HTTP over SSL/TLS)

Despite being decades old and standardized, still a host of issues

Heartbleed

SSL/TLS

HTTPS (HTTP over SSL/TLS)

Despite being decades old and standardized, still a host of issues

Heartbleed

* *Protocol:* BEAST, CRIME, LUCKY 13, Triple Handshake, RC4 attacks, Renegotiation
* *CAs:* Comodo, DigiNotar, TURKTRUST, TeliaSonera
* *Implementation:* GoTo Fail (Apple & GnuTLS)

SSL/TLS

Heartbleed

Software error in popular SSL library OpenSSL

Allowed anyone connected over HTTPS to a server can have it leak ~64KB of whatever is in memory

Passwords, social security numbers (Revenue Canada), private SSL/TLS keys (Cloudflare)

SSL/TLS

Revocation

Certificates are issued by hundreds of trusted CAs — any CA can issue a cert for any site!

Each time you visit https, you ping the CA to see if cert is still valid — fails open!

No great alternative

SSL/TLS

Primitive	Security Properties Offered						Evaluation of Impact on HTTPS									
	A				B	C	Security & Privacy				Deployability				Usability		
	Detects MITM	Detects Local MITM	Protects Client Credential	Updatable Pins	Detects TLS Stripping	Affirms POST-to-HTTPS	Responsive Revocation	Intermediate CAs Visible	No New Trusted Entity	No New Traceability	Reduces Traceability	No New Auth'n Tokens	No Server-Side Changes	Deployable without DNSSEC	No Extra Communications	Internet Scalable	No False-Rejects	Status Signalled Completely	No New User Decisions
Key Pinning (Client History)	○	○	○				●	●		●	●	●	●						
Key Pinning (Server)	○	○	○				●	●				●	●	●	●		●		●
Key Pinning (Preloaded)	●	●	●	●			○	●		●	○	●	●		●	○	●		
Key Pinning (DNS)	●	●	●	●			○	●	●		○		●	●	●	○	●		
Multipath Probing		●		●						●	●	●		●		●			
Channel-bound Credentials			○				●	●		●		●	●	●	●	○	●		
Credential-bound Channels			○				●	●		●		●	●	●	●	○	●		
Key Agility/Manifest				●			●	●				●	●	●	●	●	●		
HTTPS-only Pinning (Server)					○	○	●	●				●	●	●	●		●		
HTTPS-only Pinning (Preloaded)				●	●	●	○	●		●	○	●	●		●	○	●		
HTTPS-only Pinning (DNS)				●	●	●	○	●			○		●	●	●	○	●		
Visual Cues for Secure POST						●	●	●		●	●	●		●		●			
Browser-stored CRL						●	○	●		●	●	●	●	●	●	●	●		
Certificate Status Stapling						●	●	●	●			●	●	●	●	○	●		
Short-lived Certificates						●	●	●	●	●		●	●	●	●	●	●		
List of Active Certificates						●	●		●	●	●	●		●	●	●	●		

[*IEEE Symp on Security & Privacy 2013*]

Secure Elections

When you cast a ballot in an election, how do you know your vote counted?

How do you know every ballot in an entire country was counted correctly?

Secure Elections

When you cast a ballot in an election, how do you know your vote counted?

How do you know every ballot in an entire country was counted correctly?

We use cryptography to produce a tally that is verifiable (independent of any software) yet preserves ballot secrecy

1-392060

Stub Number:

City of Takoma Park, Maryland
MUNICIPAL ELECTION
NOVEMBER 3, 2009

OFFICIAL BALLOT — WARD 1

Instructions: Vote for candidates by indicating your first-choice candidate, your second-choice candidate, and so on. You are free to rank only a first choice if you wish.

Do not fill in more than one oval per column. Do not fill in more than one oval per candidate. Do not skip numbers in the ranking sequence.

To vote for a person whose name is not printed on the ballot, write the name in the space provided and fill in one box in the column indicating your ranking of the write-in candidate.

If you make a mistake on your ballot, return it to the judge and get another.

Do not make any identifying marks on your ballot.

When you mark an oval to rank a candidate, a code will be revealed that you may later use to verify your vote online. See the instruction sheet in the voting booth.

Ciudad de Takoma Park, Maryland
ELECCIONES MUNICIPALES
3 DE NOVIEMBRE DE 2009

BOLETA OFICIAL— DISTRITO ELECTORAL 1

Instrucciones: *Vote por los candidatos indicando el candidato que sea su primera opción, el candidato que sea su segunda opción, y así sucesivamente. Si lo desea, puede limitarse a seleccionar solamente al candidato que sea su primera opción.*

No rellene más de una casilla por cada columna. *No rellene más de una casilla por cada candidato. No salte números en la secuencia de clasificación por orden.*

Para votar por una persona cuyo nombre no esté impreso en la boleta, escriba el nombre en el espacio provisto y rellene una casilla en la columna para indicar el orden de clasificación del candidato que se ha añadido.

Si usted comete un error en su boleta, devuélvasela al juez y pida otra.

No haga marcas en su boleta que puedan identificarlo.

Cuando usted marque la casilla para votar por un candidato, verá un código que podrá usar posteriormente para verificar su voto por Internet*. Vea la hoja de instrucciones en la cabina de votación.*

MAYOR ***ALCALDE***			
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	**1st choice** **1ra** opción	**2nd choice** **2da** opción	**3rd choice** **3ra** opción
Roger B. Schlegel	⬭	⬭	⬭
Bruce Williams	⬭	⬭	⬭
Write-In Candidate/*Para añadir a un candidato*	⬭	⬭	⬭

CITY COUNCIL MEMBER WARD 1 ***MIEMBRO DEL CONSEJO DE LA CIUDAD DISTRITO ELECTORAL 1***		
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	**1st choice** **1ra** opción	**2nd choice** **2da** opción
Josh Wright	⬭	⬭
Write-In Candidate/*Para añadir a un candidato*	⬭	⬭

1-634527

Online Verification Number/
Número de Verificación por Internet

INSTRUCTIONS FOR VERIFYING YOUR VOTE ON-LINE AFTER YOU RETURN HOME
PARA LAS INSTRUCCIONES EN ESPAÑOL VEA AL DORSO

You have the **OPTION** of verifying your vote on-line after you return home. **It is not necessary to do so.** You may ignore this step entirely; **your cast ballot will be counted whether or not you do this verification.**

If you wish to verify your vote on-line, perform the following steps:
1. Fill out your ballot according to the instructions provided on the ballot. "Confirmation numbers" will appear inside the ovals you mark.
2. **BEFORE** YOU CAST YOUR BALLOT Record the Online Verification Number and the confirmation numbers below, using the narrow tip of the special pen (note that Wards 1-5 will not have a 3rd choice confirmation number for the city council race).

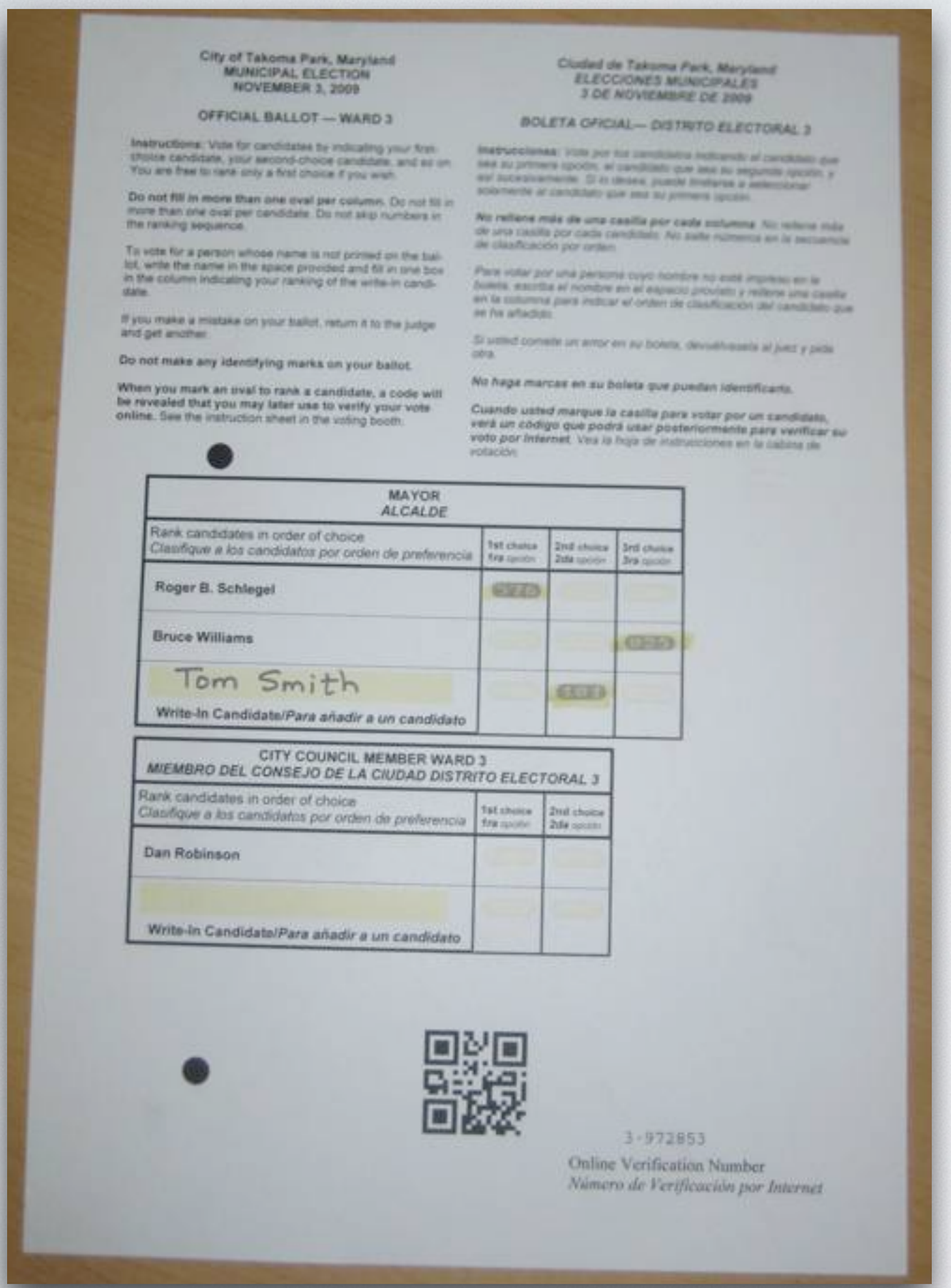
"On-Line Verification Number" from the bottom right corner of your ballot

Confirmation Numbers	1st Choice	2nd Choice	3rd Choice
Mayor			
City Council Member			

3. **Cast your ballot as usual using the poll-site scanner. DO NOT CAST THIS SHEET, but take it home with you.**
4. After you have returned home, use a computer with an Internet connection to access the City Clerk's web page: **www.takomaparkmd.gov/clerk**. Here you will see instructions for verifying that the confirmation numbers you wrote down are correctly recorded. Note that the confirmation numbers are randomly generated and cannot be used to determine your vote.

Thank you for verifying your vote!
The Takoma Park Board of Elections

[*USENIX Security 2010*]



City of Takoma Park, Maryland
MUNICIPAL ELECTION
NOVEMBER 3, 2009

OFFICIAL BALLOT — WARD 3

Instructions: Vote for candidates by indicating your first-choice candidate, your second-choice candidate, and so on. You are free to rank only a first choice if you wish.

Do not fill in more than one oval per column. Do not fill in more than one oval per candidate. Do not skip numbers in the ranking sequence.

To vote for a person whose name is not printed on the ballot, write the name in the space provided and fill in one box in the column indicating your ranking of the write-in candidate.

If you make a mistake on your ballot, return it to the judge and get another.

Do not make any identifying marks on your ballot.

When you mark an oval to rank a candidate, a code will be revealed that you may later use to verify your vote online. See the instruction sheet in the voting booth.

Ciudad de Takoma Park, Maryland
ELECCIONES MUNICIPALES
3 DE NOVIEMBRE DE 2009

BOLETA OFICIAL— DISTRITO ELECTORAL 3

Instrucciones: *Vote por los candidatos indicando el candidato que sea su primera opción, el candidato que sea su segunda opción, y así sucesivamente. Si lo desea, puede limitarse a seleccionar solamente el candidato que sea su primera opción.*

No rellene más de una casilla por cada columna. *No rellene más de una casilla por cada candidato. No salte números en la secuencia de clasificación por orden.*

Para votar por una persona cuyo nombre no está impreso en la boleta, escriba el nombre en el espacio provisto y rellene una casilla en la columna para indicar el orden de clasificación del candidato que se ha añadido.

Si usted comete un error en su boleta, devuélvasela al juez y pida otra.

No haga marcas en su boleta que puedan identificarla.

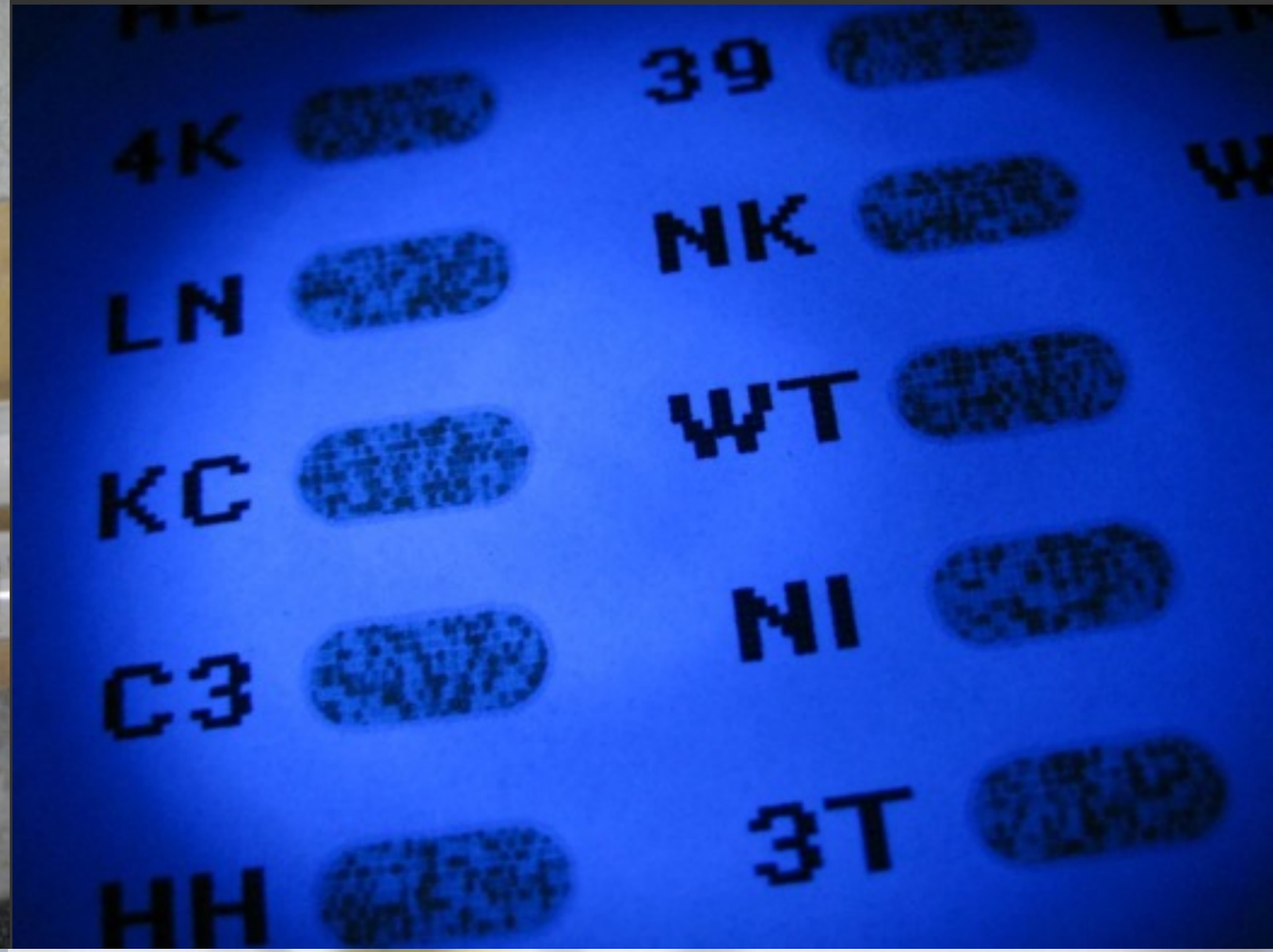
Cuando usted marque la casilla para votar por un candidato, verá un código que podrá usar posteriormente para verificar su voto por Internet. *Vea la hoja de instrucciones en la cabina de votación.*

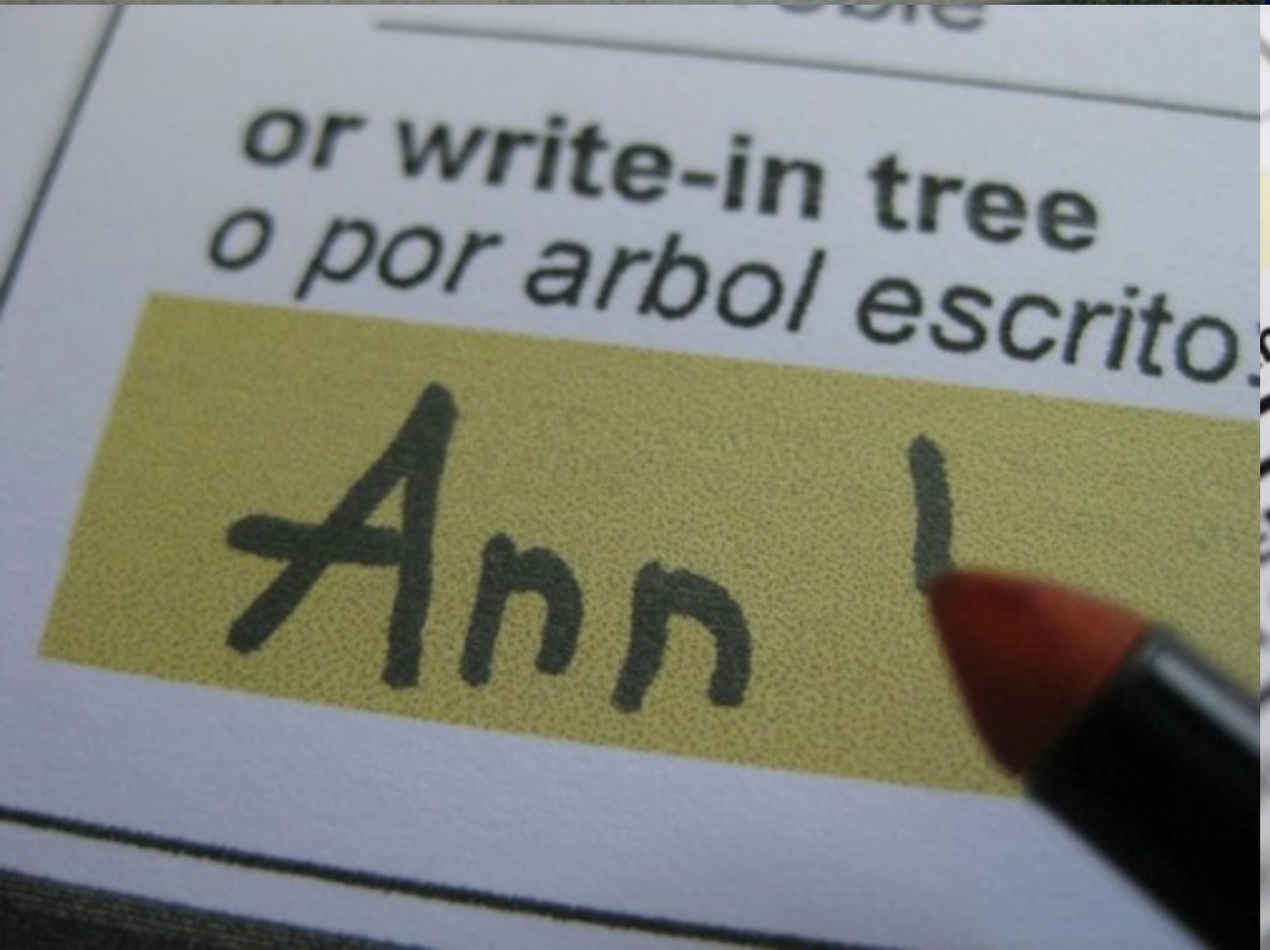
MAYOR *ALCALDE*			
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice *1ra opción*	2nd choice *2da opción*	3rd choice *3ra opción*
Roger B. Schlegel			
Bruce Williams			
Tom Smith Write-In Candidate/*Para añadir a un candidato*			

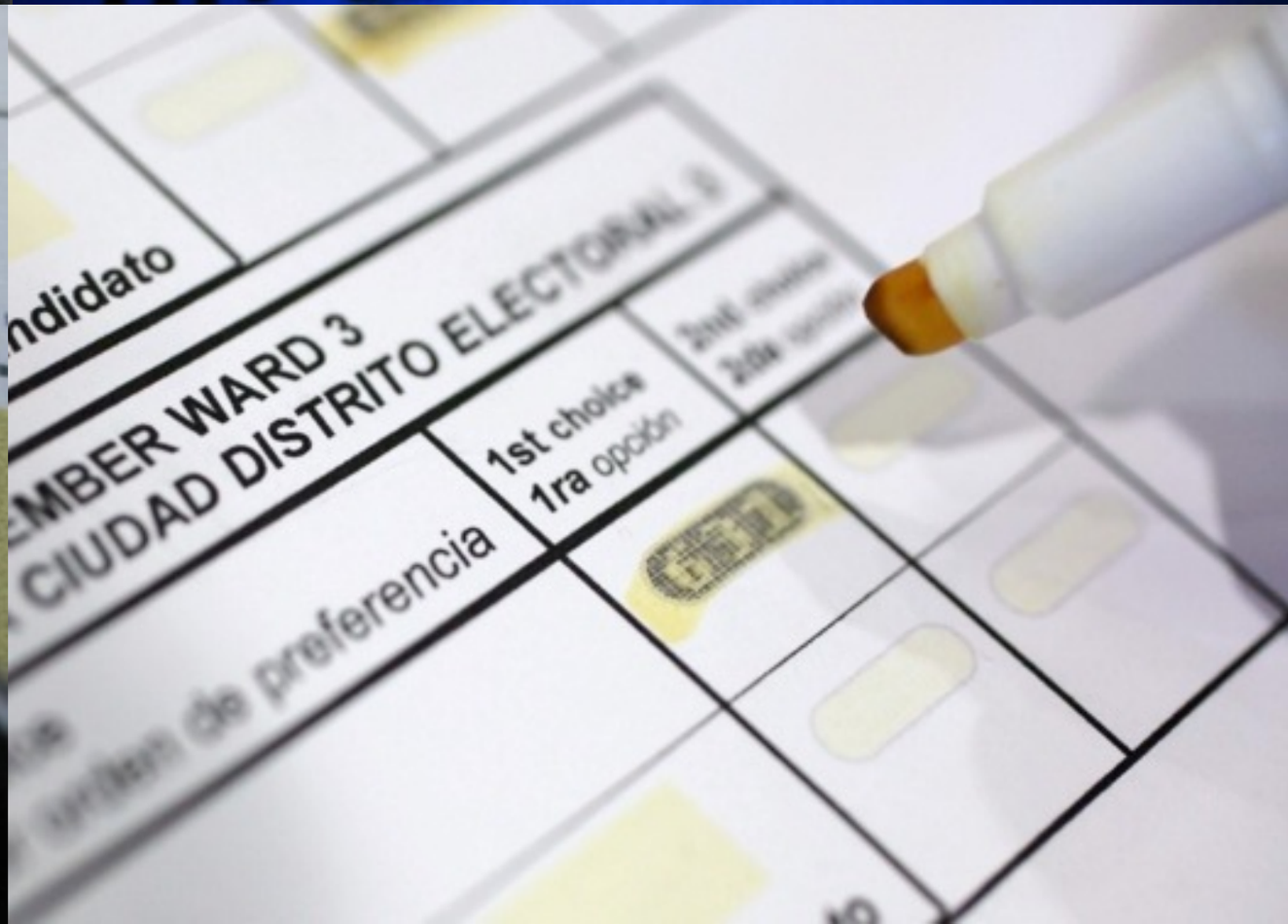
CITY COUNCIL MEMBER WARD 3 *MIEMBRO DEL CONSEJO DE LA CIUDAD DISTRITO ELECTORAL 3*		
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice *1ra opción*	2nd choice *2da opción*
Dan Robinson		
Write-In Candidate/*Para añadir a un candidato*		

3-972853
Online Verification Number
Número de Verificación por Internet

[*USENIX Security 2010*]


39
4K
NK
LN
WT
KC
NI
C3
3T
HH


or write-in tree
o por arbol escrito
Ann


ndidato
EMBER WARD 3
CIUDAD DISTRITO ELECTORAL 3
1st choice
1ra opción
de preferencia

Secure Elections

Internet Voting — the new frontier

Secure Elections

Internet Voting — the new frontier

What if voters have malware on their computers?
[*ACNS 2013*]

What if voters sell their passwords or are coerced in-person to vote a certain way?
[*USENIX HotSec 2008, FC 2011, USENIX EVT/WOTE 2012*]

Bitcoin

Bitcoin is a digital cryptographic currency with a 5B USD market cap

Bitcoin

Bitcoin is a digital cryptographic currency with a 5B USD market cap

Is the value real?

Should it be regulated? Taxed?

Is it a threat for money laundering or other crime?

Bitcoin

Bitcoin is a digital cryptographic currency with a 5B USD market cap

Enables 24/7 international digital transactions that *settle* within minutes and have low fees

Email for money

Programmable money

Bitcoin

Decentralization: No one is in charged, difficult to disrupt

The consensus mechanism can be repurposed for other interesting things: strong timestamping and decentralized markets

[*FC 2012, FC 2014, WEIS 2014*]

SSL/TLS

Election Security

Bitcoin

Genomic Privacy

Android Security

Financial Market Security

Thank You

Questions?