

# A Modification of Punchscan: Trust Distribution

Przemysław Kubiak

Institute of Mathematics and Computer Science,  
Wrocław University of Technology

Frontiers in Electronic Elections,  
September 19, 2006

# Outline

## An Overview of Punchscan

### **Features**

### **The Voting Ballot**

### **The Election Process**

## The Modification

### **The Ballot**

### **“Maths” Behind Ballots**

### **The Election Process**

## $L = 2$ and the Original Punchscan

## Final Remarks

# Punchscan features

- ▶ Hybrid paper-electronic election scheme (no voting machines – very transparent),

# Punchscan features

- ▶ Hybrid paper-electronic election scheme (no voting machines – very transparent),
- ▶ Effective and particularly simple for a voter,

# Punchscan features

- ▶ Hybrid paper-electronic election scheme (no voting machines – very transparent),
- ▶ Effective and particularly simple for a voter,
- ▶ Verifiable,

# Punchscan features

- ▶ Hybrid paper-electronic election scheme (no voting machines – very transparent),
- ▶ Effective and particularly simple for a voter,
- ▶ Verifiable,
- ▶ There is a single Election Authority, which knows links between ballot serial numbers and the votes.

5134

D 0. Nihilist  
 E 1. Buddhist  
 A 2. Anarchist  
 B 3. Sophist  
 C 4. Solipsist

(E) (A) (B) (C) (D)

5134

D 0. Nihilist  
 E 1. Buddhist  
 A 2. Anarchist  
 B 3. Sophist  
 C 4. Solipsist

○ ○ (A) ○ ○ ○

5134

0	1	2	3	4
E	(A)	B	C	D

$c \in \{0, \dots, n-1\}$  – candidate's index  
 $r \in \{0, \dots, n-1\}$  – index of the mark

$s_1, s_2$  – shifts of the letters

$c = 2, r = 1, s_1 = 3, s_2 = 4$

$c + s_1 = r + s_2 \pmod n$

Let  $k$  be a ballot serial number ( $k = 5134$  in the example).  
Before election, for each  $k$  Election Authority publishes:

Let  $k$  be a ballot serial number ( $k = 5134$  in the example).  
Before election, for each  $k$  Election Authority publishes:

- ▶ commitments  $C(s_1^{(k)})$ ,  $C(s_2^{(k)})$ ,

Let  $k$  be a ballot serial number ( $k = 5134$  in the example).  
Before election, for each  $k$  Election Authority publishes:

- ▶ commitments  $C(s_1^{(k)})$ ,  $C(s_2^{(k)})$ ,
- ▶ empty result table  $R: [i, \bullet]$ ,  
and empty table of partial results  $R': [j, \bullet]$ ,

Let  $k$  be a ballot serial number ( $k = 5134$  in the example).  
Before election, for each  $k$  Election Authority publishes:

- ▶ commitments  $C(s_1^{(k)})$ ,  $C(s_2^{(k)})$ ,
- ▶ empty result table  $R$ :  $[i, \bullet]$ ,  
and empty table of partial results  $R'$ :  $[j, \bullet]$ ,
- ▶ decryption table with commitments  $C(\tilde{s}_1^{(k)})$ ,  $C(\tilde{s}_2^{(k)})$ ,  
( $\tilde{s}_1^{(k)}$  is random,  $-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod n$ ),

With the decryption table two secret permutations  $\pi_1$ ,  $\pi_2$  are associated.

Let  $k$  be a ballot serial number ( $k = 5134$  in the example).  
Before election, for each  $k$  Election Authority publishes:

- ▶ commitments  $C(s_1^{(k)})$ ,  $C(s_2^{(k)})$ ,
- ▶ empty result table  $R$ :  $[i, \bullet]$ ,  
and empty table of partial results  $R'$ :  $[j, \bullet]$ ,
- ▶ decryption table with commitments  $C(\tilde{s}_1^{(k)})$ ,  $C(\tilde{s}_2^{(k)})$ ,  
( $\tilde{s}_1^{(k)}$  is random,  $-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod n$ ),

With the decryption table two secret permutations  $\pi_1$ ,  $\pi_2$  are associated.

After election:

Let  $k$  be a ballot serial number ( $k = 5134$  in the example).  
Before election, for each  $k$  Election Authority publishes:

- ▶ commitments  $C(s_1^{(k)}), C(s_2^{(k)})$ ,
- ▶ empty result table  $R: [i, \bullet]$ ,  
and empty table of partial results  $R': [j, \bullet]$ ,
- ▶ decryption table with commitments  $C(\tilde{s}_1^{(k)}), C(\tilde{s}_2^{(k)})$ ,  
( $\tilde{s}_1^{(k)}$  is random,  $-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod n$ ),

With the decryption table two secret permutations  $\pi_1, \pi_2$  are associated.

After election:

- ▶  $(k, r^{(k)})$  are published,

Let  $k$  be a ballot serial number ( $k = 5134$  in the example).  
Before election, for each  $k$  Election Authority publishes:

- ▶ commitments  $C(s_1^{(k)})$ ,  $C(s_2^{(k)})$ ,
- ▶ empty result table  $R$ :  $[i, \bullet]$ ,  
and empty table of partial results  $R'$ :  $[j, \bullet]$ ,
- ▶ decryption table with commitments  $C(\tilde{s}_1^{(k)})$ ,  $C(\tilde{s}_2^{(k)})$ ,  
( $\tilde{s}_1^{(k)}$  is random,  $-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod n$ ),

With the decryption table two secret permutations  $\pi_1$ ,  $\pi_2$  are associated.

After election:

- ▶  $(k, r^{(k)})$  are published,
- ▶  $C(s_v^{(k)})$  are opened,  $v$  - not destroyed layer,

Let  $k$  be a ballot serial number ( $k = 5134$  in the example).  
Before election, for each  $k$  Election Authority publishes:

- ▶ commitments  $C(s_1^{(k)})$ ,  $C(s_2^{(k)})$ ,
- ▶ empty result table  $R$ :  $[i, \bullet]$ ,  
and empty table of partial results  $R'$ :  $[j, \bullet]$ ,
- ▶ decryption table with commitments  $C(\tilde{s}_1^{(k)})$ ,  $C(\tilde{s}_2^{(k)})$ ,  
( $\tilde{s}_1^{(k)}$  is random,  $-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod n$ ),

With the decryption table two secret permutations  $\pi_1$ ,  $\pi_2$  are associated.

After election:

- ▶  $(k, r^{(k)})$  are published,
- ▶  $C(s_v^{(k)})$  are opened,  $v$  - not destroyed layer,
- ▶ Tables  $R$ ,  $R'$  are filled in:  $R'$  with  $[\pi_1(k), r^{(k)} - \tilde{s}_1^{(k)} \pmod n]$ ,  
 $R$  with  $[\pi_2(\pi_1(k)), r^{(k)} - \tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} \pmod n]$ .

## Audits:

- ▶ Pre-election: for half of the ballots congruence  $-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod n$  is verified.

## Audits:

- ▶ Pre-election: for half of the ballots congruence  $-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod n$  is verified.
- ▶ Post-election:

## Audits:

- ▶ Pre-election: for half of the ballots congruence

$$-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod{n} \text{ is verified.}$$

- ▶ Post-election:

1. for a random  $t \in \{1, 2\}$  and for all ballots  $k$  commitments  $C(\tilde{s}_t^{(k)})$  are opened and  $\pi_t$  is revealed,

## Audits:

- ▶ Pre-election: for half of the ballots congruence  $-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod n$  is verified.
- ▶ Post-election:
  1. for a random  $t \in \{1, 2\}$  and for all ballots  $k$  commitments  $C(\tilde{s}_t^{(k)})$  are opened and  $\pi_t$  is revealed,
  2. there are many decryption tables, each one with independent  $\tilde{s}_1^{(k)}$ ,  $\pi_1$ , and with separate  $R'$  (for each table the choice of  $t$  is repeated),

## Audits:

- ▶ Pre-election: for half of the ballots congruence  $-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod n$  is verified.
- ▶ Post-election:
  1. for a random  $t \in \{1, 2\}$  and for all ballots  $k$  commitments  $C(\tilde{s}_t^{(k)})$  are opened and  $\pi_t$  is revealed,
  2. there are many decryption tables, each one with independent  $\tilde{s}_1^{(k)}$ ,  $\pi_1$ , and with separate  $R'$  (for each table the choice of  $t$  is repeated),  $\tilde{s}_2^{(k)}$  is determined by  $\tilde{s}_1^{(k)}$ ,  $\pi_2$  by  $\pi_1$  and the order in  $R$ ,  $R'$  is determined by  $\pi_1$ , values of  $r^{(k)}$  and shifts.

## Audits:

- ▶ Pre-election: for half of the ballots congruence  $-\tilde{s}_1^{(k)} + \tilde{s}_2^{(k)} = -s_1^{(k)} + s_2^{(k)} \pmod n$  is verified.
- ▶ Post-election:
  1. for a random  $t \in \{1, 2\}$  and for all ballots  $k$  commitments  $C(\tilde{s}_t^{(k)})$  are opened and  $\pi_t$  is revealed,
  2. there are many decryption tables, each one with independent  $\tilde{s}_1^{(k)}$ ,  $\pi_1$ , and with separate  $R'$  (for each table the choice of  $t$  is repeated),  $\tilde{s}_2^{(k)}$  is determined by  $\tilde{s}_1^{(k)}$ ,  $\pi_2$  by  $\pi_1$  and the order in  $R$ ,  $R'$  is determined by  $\pi_1$ , values of  $r^{(k)}$  and shifts.

EA knows the link  $k \rightarrow c^{(k)}$  !

# Outline

An Overview of Punchscan

**Features**

**The Voting Ballot**

**The Election Process**

**The Modification**

**The Ballot**

**"Maths" Behind Ballots**

**The Election Process**

$L = 2$  and the Original Punchscan

Final Remarks

I:

0	1	2	3	4
2	3	4	0	1

$k = 5134$ , shift = 2

II:

0	1	2	3	4
4	0	1	2	3

$k = 5134$ , shift = 4

III:

0	1	2	3	4
3	4	0	1	2

$k = 5134$ , shift = 3

→

0. Nihilist
1. Buddhist
2. Anarchist
3. Sophist
4. Solipsist

IV:

0	1	2	3	4
2	3	4	0	1

$k = 5134$ , shift = 2

AG:

5134:				
0	1	2	3	4

A multilayer ballot (four layers and an answer grid).

Voters might write on the layers. Is it more complicated than e.g. the Neff's scheme?

Let

- ▶  $L$  be a number of layers,
- ▶  $c$  be a candidate's index,
- ▶  $s_\ell$  be a shift in the  $\ell$ th layer in the set.

Let

- ▶  $L$  be a number of layers,
- ▶  $c$  be a candidate's index,
- ▶  $s_\ell$  be a shift in the  $\ell$ th layer in the set.

Then in the Answer Grid (AG) is put

$$r = c + \sum_{\ell=1}^L s_\ell \pmod n$$

(addition is commutative – layers can be used in any order).

Let

- ▶  $L$  be a number of layers,
- ▶  $c$  be a candidate's index,
- ▶  $s_\ell$  be a shift in the  $\ell$ th layer in the set.

Then in the Answer Grid (AG) is put

$$r = c + \sum_{\ell=1}^L s_\ell \pmod n$$

(addition is commutative – layers can be used in any order).

For  $\ell$ th layer is responsible a separate authority  $A_\ell$ .

Let

- ▶  $L$  be a number of layers,
- ▶  $c$  be a candidate's index,
- ▶  $s_\ell$  be a shift in the  $\ell$ th layer in the set.

Then in the Answer Grid (AG) is put

$$r = c + \sum_{\ell=1}^L s_\ell \pmod n$$

(addition is commutative – layers can be used in any order).

For  $\ell$ th layer is responsible a separate authority  $A_\ell$ .

The (simplified) commitment to  $s_\ell$  is

$$E(-s_\ell) = (g^{\beta_\ell}, g^{-s_\ell} \cdot Y_T^{\beta_\ell})$$

where  $Y_T$  is a product of public keys of tellers.

The crucial feature for shifts addition with the layers is additivity in the onions' exponent:

$$\prod_{\ell=1}^L E(-s_{\ell}) = (g^{\sum_{\ell=1}^L \beta_{\ell}}, g^{\sum_{\ell=1}^L -s_{\ell}} \cdot Y_T^{\sum_{\ell=1}^L \beta_{\ell}})$$

The crucial feature for shifts addition with the layers is additivity in the onions' exponent:

$$\prod_{\ell=1}^L E(-s_{\ell}) = (g^{\sum_{\ell=1}^L \beta_{\ell}}, g^{\sum_{\ell=1}^L -s_{\ell}} \cdot Y_T^{\sum_{\ell=1}^L \beta_{\ell}})$$

So having  $r$  from the AG we multiply  $g^r$  into the onion:

$$(g^{\sum_{\ell=1}^L \beta_{\ell}}, g^{r + (\sum_{\ell=1}^L -s_{\ell})} \cdot Y_T^{\sum_{\ell=1}^L \beta_{\ell}}).$$

as in one of PaV versions.

The crucial feature for shifts addition with the layers is additivity in the onions' exponent:

$$\prod_{\ell=1}^L E(-s_\ell) = (g^{\sum_{\ell=1}^L \beta_\ell}, g^{\sum_{\ell=1}^L -s_\ell} \cdot Y_T^{\sum_{\ell=1}^L \beta_\ell})$$

So having  $r$  from the AG we multiply  $g^r$  into the onion:

$$(g^{\sum_{\ell=1}^L \beta_\ell}, g^{r+(\sum_{\ell=1}^L -s_\ell)} \cdot Y_T^{\sum_{\ell=1}^L \beta_\ell}).$$

as in one of PaV versions. After decryption by the tellers we get

$$g^{r+(\sum_{\ell=1}^L -s_\ell)}.$$

The crucial feature for shifts addition with the layers is additivity in the onions' exponent:

$$\prod_{\ell=1}^L E(-s_\ell) = (g^{\sum_{\ell=1}^L \beta_\ell}, g^{\sum_{\ell=1}^L -s_\ell} \cdot Y_T^{\sum_{\ell=1}^L \beta_\ell})$$

So having  $r$  from the AG we multiply  $g^r$  into the onion:

$$(g^{\sum_{\ell=1}^L \beta_\ell}, g^{r+(\sum_{\ell=1}^L -s_\ell)} \cdot Y_T^{\sum_{\ell=1}^L \beta_\ell}).$$

as in one of PaV versions. After decryption by the tellers we get

$$g^{r+(\sum_{\ell=1}^L -s_\ell)}.$$

Denote  $r + (\sum_{\ell=1}^L -s_\ell)$  by  $x$ .  $|x|$  is small (easy to calculate).  
The vote equals  $c = x \bmod n$ .

There are two (not necessarily different) sets of authorities: tellers, and clerks  $A_\ell$ ,  $\ell = 1, \dots, L$ .

Election process (sketch):

There are two (not necessarily different) sets of authorities: tellers, and clerks  $A_\ell$ ,  $\ell = 1, \dots, L$ .

Election process (sketch):

- ▶ Commitments  $E(-s_\ell) = (g^{\beta_\ell}, g^{-s_\ell} \cdot Y_T^{\beta_\ell})$  are made.

There are two (not necessarily different) sets of authorities: tellers, and clerks  $A_\ell$ ,  $\ell = 1, \dots, L$ .

Election process (sketch):

- ▶ Commitments  $E(-s_\ell) = (g^{\beta_\ell}, g^{-s_\ell} \cdot Y_T^{\beta_\ell})$  are made.
- ▶ Voting phase:
  1. a voter is given two sets of (folded) layers (each set has its unique serial number  $k$ ),

There are two (not necessarily different) sets of authorities: tellers, and clerks  $A_\ell$ ,  $\ell = 1, \dots, L$ .

Election process (sketch):

- ▶ Commitments  $E(-s_\ell) = (g^{\beta_\ell}, g^{-s_\ell} \cdot Y_T^{\beta_\ell})$  are made.
- ▶ Voting phase:
  1. a voter is given two sets of (folded) layers (each set has its unique serial number  $k$ ),
  2. a voter indicates one set for verification,

There are two (not necessarily different) sets of authorities: tellers, and clerks  $A_\ell$ ,  $\ell = 1, \dots, L$ .

Election process (sketch):

- ▶ Commitments  $E(-s_\ell) = (g^{\beta_\ell}, g^{-s_\ell} \cdot Y_T^{\beta_\ell})$  are made.
- ▶ Voting phase:
  1. a voter is given two sets of (folded) layers (each set has its unique serial number  $k$ ),
  2. a voter indicates one set for verification,
  3. the other set is used to "calculate"  $r$  and the layers are destroyed (so the voters can write on them during  $r$  "calculation"),

There are two (not necessarily different) sets of authorities: tellers, and clerks  $A_\ell$ ,  $\ell = 1, \dots, L$ .

Election process (sketch):

- ▶ Commitments  $E(-s_\ell) = (g^{\beta_\ell}, g^{-s_\ell} \cdot Y_T^{\beta_\ell})$  are made.
- ▶ Voting phase:
  1. a voter is given two sets of (folded) layers (each set has its unique serial number  $k$ ),
  2. a voter indicates one set for verification,
  3. the other set is used to "calculate"  $r$  and the layers are destroyed (so the voters can write on them during  $r$  "calculation"),
  4.  $r$  with the corresponding serial number goes on the bulletin board.

There are two (not necessarily different) sets of authorities: tellers, and clerks  $A_\ell$ ,  $\ell = 1, \dots, L$ .

Election process (sketch):

- ▶ Commitments  $E(-s_\ell) = (g^{\beta_\ell}, g^{-s_\ell} \cdot Y_T^{\beta_\ell})$  are made.
- ▶ Voting phase:
  1. a voter is given two sets of (folded) layers (each set has its unique serial number  $k$ ),
  2. a voter indicates one set for verification,
  3. the other set is used to "calculate"  $r$  and the layers are destroyed (so the voters can write on them during  $r$  "calculation"),
  4.  $r$  with the corresponding serial number goes on the bulletin board.
- ▶ Onions are made and the mixing phase begins.

# Outline

An Overview of Punchscan

**Features**

**The Voting Ballot**

**The Election Process**

The Modification

**The Ballot**

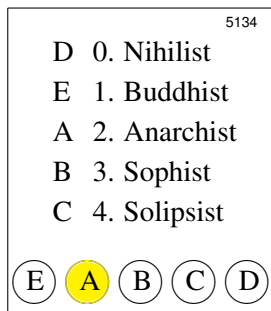
**“Maths” Behind Ballots**

**The Election Process**

$L = 2$  and the Original Punchscan

Final Remarks

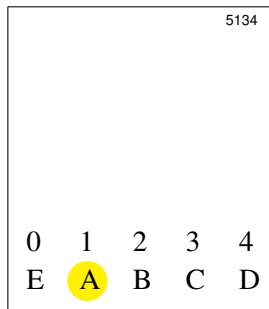
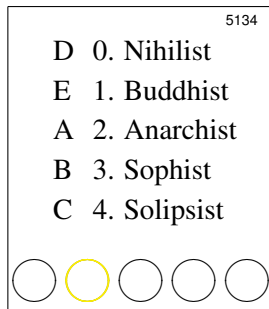
# Trust distribution between two authorities



$$c + s_1 = r + s_2 \pmod{n}$$

$$c = r + s_2 - s_1 \pmod{n}$$

Commitments:  $E(s_2)$ ,  $E(-s_1)$ ,  
both layers must be destroyed!  
(e.g. each by its issuer)



# Outline

An Overview of Punchscan

**Features**

**The Voting Ballot**

**The Election Process**

The Modification

**The Ballot**

**“Maths” Behind Ballots**

**The Election Process**

$L = 2$  and the Original Punchscan

**Final Remarks**

- ▶ Hybrid paper-electronic schemes seem to be more transparent than purely electronic ones (cf. Diebold AccuVote-TS).

- ▶ Hybrid paper-electronic schemes seem to be more transparent than purely electronic ones (cf. Diebold AccuVote-TS).
- ▶ Punchscan and PaV preserve traditional way of marking a vote.

- ▶ Hybrid paper-electronic schemes seem to be more transparent than purely electronic ones (cf. Diebold AccuVote-TS).
- ▶ Punchscan and PaV preserve traditional way of marking a vote.
- ▶ If we allow to change voters actions slightly, the protocol may gain a new functionality: trust distribution, and for  $L > 2$  resistance to collusion of two clerks.

- ▶ Hybrid paper-electronic schemes seem to be more transparent than purely electronic ones (cf. Diebold AccuVote-TS).
- ▶ Punchscan and PaV preserve traditional way of marking a vote.
- ▶ If we allow to change voters actions slightly, the protocol may gain a new functionality: trust distribution, and for  $L > 2$  resistance to collusion of two clerks.
- ▶ For  $L = 2$  the simplicity of the original scheme is preserved.

- ▶ Hybrid paper-electronic schemes seem to be more transparent than purely electronic ones (cf. Diebold AccuVote-TS).
- ▶ Punchscan and PaV preserve traditional way of marking a vote.
- ▶ If we allow to change voters actions slightly, the protocol may gain a new functionality: trust distribution, and for  $L > 2$  resistance to collusion of two clerks.
- ▶ For  $L = 2$  the simplicity of the original scheme is preserved.
- ▶ Other enhancements are possible (e.g. permutations instead of shifts).

# Thanks for your attention