

Verifying complex ballots with a single (constant size) verification code

Rui Joaquim
rui.joaquim@uni.lu

Introduction

- The verification of a vote encryption is needed to:
 - Guarantee that a valid vote is encrypted.
 - Important for both mix-net and homomorphic tallying.
 - Guarantee that the voter's choice is encrypted correctly.
 - Important for cast-as-intended and end-to-end verifiability.
- A complex ballot is one that has a large number of valid vote possibilities.

Complex ballot example 1

Darmstadt, Germany

Stimmzettel
für die Wahl zur Stadtverordnetenversammlung der Wissenschaftsstadt Darmstadt am 26. März 2006

Sie haben 71 Stimmen!

• Sie können alle 71 Stimmen an verschiedene Bewerberinnen und Bewerber in verschiedenen Wahlvorschlägen vergeben – **parieren** – und über jeder Person auf dem Stimmzettel bis zu drei Stimmen geben – **kumulieren** – (S. 1, 2, 3 oder 5, 6, 7).

• Sie können, wenn Sie nicht alle 71 Stimmen einzeln vergeben wollen oder noch Stimmen übrig haben, **zusätzlich einen Wahlvorschlag in der Kopfzeile** kennzeichnen ☐. In diesem Fall hat das Ankreuzen der Kopfzeile zur Folge, dass alle 71 Stimmen vergeben und Bewerber des betreffenden Wahlvorschlags in der Reihenfolge ihrer Benennung so lange eine weitere Stimme zugerechnet wird, bis alle Stimmen verbraucht sind.

• Sie können einen **Wahlvorschlag** auch nur in der **Kopfzeile** kennzeichnen ☐, ohne Stimmen an Personen zu vergeben. Das hat zur Folge, dass jede Person in der Reihenfolge des Wahlvorschlags so lange jeweils eine Stimme erhält, bis alle 71 Stimmen vergeben oder jeder Person des Wahlvorschlags drei Stimmen zugerechnet sind.

• Falls Sie einen Wahlvorschlag in der Kopfzeile kennzeichnen, können Sie auch Bewerberinnen und Bewerber in diesem Wahlvorschlag **streichen**, dessen Personen werden dann keine Stimmen zugerechnet.

Mann, geboren 1947 bis 1961

Bitte Stimmzettel nach innen falten

1 Christlich Demokratische Union Deutschlands
CDU

101	Andreas Müller
102	Christoph Müller
103	Ulrich Müller
104	Ulrich Müller
105	Ulrich Müller
106	Ulrich Müller
107	Ulrich Müller
108	Ulrich Müller
109	Ulrich Müller
110	Ulrich Müller
111	Ulrich Müller
112	Ulrich Müller
113	Ulrich Müller
114	Ulrich Müller
115	Ulrich Müller
116	Ulrich Müller
117	Ulrich Müller
118	Ulrich Müller
119	Ulrich Müller
120	Ulrich Müller
121	Ulrich Müller
122	Ulrich Müller
123	Ulrich Müller
124	Ulrich Müller
125	Ulrich Müller
126	Ulrich Müller
127	Ulrich Müller
128	Ulrich Müller
129	Ulrich Müller
130	Ulrich Müller
131	Ulrich Müller
132	Ulrich Müller
133	Ulrich Müller
134	Ulrich Müller
135	Ulrich Müller
136	Ulrich Müller
137	Ulrich Müller
138	Ulrich Müller
139	Ulrich Müller
140	Ulrich Müller
141	Ulrich Müller
142	Ulrich Müller
143	Ulrich Müller
144	Ulrich Müller
145	Ulrich Müller
146	Ulrich Müller
147	Ulrich Müller
148	Ulrich Müller
149	Ulrich Müller
150	Ulrich Müller
151	Ulrich Müller
152	Ulrich Müller
153	Ulrich Müller
154	Ulrich Müller
155	Ulrich Müller
156	Ulrich Müller
157	Ulrich Müller
158	Ulrich Müller
159	Ulrich Müller
160	Ulrich Müller
161	Ulrich Müller
162	Ulrich Müller
163	Ulrich Müller
164	Ulrich Müller
165	Ulrich Müller
166	Ulrich Müller
167	Ulrich Müller
168	Ulrich Müller
169	Ulrich Müller
170	Ulrich Müller
171	Ulrich Müller
172	Ulrich Müller
173	Ulrich Müller
174	Ulrich Müller
175	Ulrich Müller
176	Ulrich Müller
177	Ulrich Müller
178	Ulrich Müller
179	Ulrich Müller
180	Ulrich Müller
181	Ulrich Müller
182	Ulrich Müller
183	Ulrich Müller
184	Ulrich Müller
185	Ulrich Müller
186	Ulrich Müller
187	Ulrich Müller
188	Ulrich Müller
189	Ulrich Müller
190	Ulrich Müller
191	Ulrich Müller
192	Ulrich Müller
193	Ulrich Müller
194	Ulrich Müller
195	Ulrich Müller
196	Ulrich Müller
197	Ulrich Müller
198	Ulrich Müller
199	Ulrich Müller
200	Ulrich Müller

2 Sozialdemokratische Partei Deutschlands
SPD

201	Ulrich Müller
202	Ulrich Müller
203	Ulrich Müller
204	Ulrich Müller
205	Ulrich Müller
206	Ulrich Müller
207	Ulrich Müller
208	Ulrich Müller
209	Ulrich Müller
210	Ulrich Müller
211	Ulrich Müller
212	Ulrich Müller
213	Ulrich Müller
214	Ulrich Müller
215	Ulrich Müller
216	Ulrich Müller
217	Ulrich Müller
218	Ulrich Müller
219	Ulrich Müller
220	Ulrich Müller
221	Ulrich Müller
222	Ulrich Müller
223	Ulrich Müller
224	Ulrich Müller
225	Ulrich Müller
226	Ulrich Müller
227	Ulrich Müller
228	Ulrich Müller
229	Ulrich Müller
230	Ulrich Müller
231	Ulrich Müller
232	Ulrich Müller
233	Ulrich Müller
234	Ulrich Müller
235	Ulrich Müller
236	Ulrich Müller
237	Ulrich Müller
238	Ulrich Müller
239	Ulrich Müller
240	Ulrich Müller
241	Ulrich Müller
242	Ulrich Müller
243	Ulrich Müller
244	Ulrich Müller
245	Ulrich Müller
246	Ulrich Müller
247	Ulrich Müller
248	Ulrich Müller
249	Ulrich Müller
250	Ulrich Müller
251	Ulrich Müller
252	Ulrich Müller
253	Ulrich Müller
254	Ulrich Müller
255	Ulrich Müller
256	Ulrich Müller
257	Ulrich Müller
258	Ulrich Müller
259	Ulrich Müller
260	Ulrich Müller
261	Ulrich Müller
262	Ulrich Müller
263	Ulrich Müller
264	Ulrich Müller
265	Ulrich Müller
266	Ulrich Müller
267	Ulrich Müller
268	Ulrich Müller
269	Ulrich Müller
270	Ulrich Müller
271	Ulrich Müller
272	Ulrich Müller
273	Ulrich Müller
274	Ulrich Müller
275	Ulrich Müller
276	Ulrich Müller
277	Ulrich Müller
278	Ulrich Müller
279	Ulrich Müller
280	Ulrich Müller
281	Ulrich Müller
282	Ulrich Müller
283	Ulrich Müller
284	Ulrich Müller
285	Ulrich Müller
286	Ulrich Müller
287	Ulrich Müller
288	Ulrich Müller
289	Ulrich Müller
290	Ulrich Müller
291	Ulrich Müller
292	Ulrich Müller
293	Ulrich Müller
294	Ulrich Müller
295	Ulrich Müller
296	Ulrich Müller
297	Ulrich Müller
298	Ulrich Müller
299	Ulrich Müller
300	Ulrich Müller

3 Bündnis 90/DIE GRÜNEN
GRÜNE

301	Ulrich Müller
302	Ulrich Müller
303	Ulrich Müller
304	Ulrich Müller
305	Ulrich Müller
306	Ulrich Müller
307	Ulrich Müller
308	Ulrich Müller
309	Ulrich Müller
310	Ulrich Müller
311	Ulrich Müller
312	Ulrich Müller
313	Ulrich Müller
314	Ulrich Müller
315	Ulrich Müller
316	Ulrich Müller
317	Ulrich Müller
318	Ulrich Müller
319	Ulrich Müller
320	Ulrich Müller
321	Ulrich Müller
322	Ulrich Müller
323	Ulrich Müller
324	Ulrich Müller
325	Ulrich Müller
326	Ulrich Müller
327	Ulrich Müller
328	Ulrich Müller
329	Ulrich Müller
330	Ulrich Müller
331	Ulrich Müller
332	Ulrich Müller
333	Ulrich Müller
334	Ulrich Müller
335	Ulrich Müller
336	Ulrich Müller
337	Ulrich Müller
338	Ulrich Müller
339	Ulrich Müller
340	Ulrich Müller
341	Ulrich Müller
342	Ulrich Müller
343	Ulrich Müller
344	Ulrich Müller
345	Ulrich Müller
346	Ulrich Müller
347	Ulrich Müller
348	Ulrich Müller
349	Ulrich Müller
350	Ulrich Müller
351	Ulrich Müller
352	Ulrich Müller
353	Ulrich Müller
354	Ulrich Müller
355	Ulrich Müller
356	Ulrich Müller
357	Ulrich Müller
358	Ulrich Müller
359	Ulrich Müller
360	Ulrich Müller
361	Ulrich Müller
362	Ulrich Müller
363	Ulrich Müller
364	Ulrich Müller
365	Ulrich Müller
366	Ulrich Müller
367	Ulrich Müller
368	Ulrich Müller
369	Ulrich Müller
370	Ulrich Müller
371	Ulrich Müller
372	Ulrich Müller
373	Ulrich Müller
374	Ulrich Müller
375	Ulrich Müller
376	Ulrich Müller
377	Ulrich Müller
378	Ulrich Müller
379	Ulrich Müller
380	Ulrich Müller
381	Ulrich Müller
382	Ulrich Müller
383	Ulrich Müller
384	Ulrich Müller
385	Ulrich Müller
386	Ulrich Müller
387	Ulrich Müller
388	Ulrich Müller
389	Ulrich Müller
390	Ulrich Müller
391	Ulrich Müller
392	Ulrich Müller
393	Ulrich Müller
394	Ulrich Müller
395	Ulrich Müller
396	Ulrich Müller
397	Ulrich Müller
398	Ulrich Müller
399	Ulrich Müller
400	Ulrich Müller

4 Freie Demokratische Partei
FDP

401	Ulrich Müller
402	Ulrich Müller
403	Ulrich Müller
404	Ulrich Müller
405	Ulrich Müller
406	Ulrich Müller
407	Ulrich Müller
408	Ulrich Müller
409	Ulrich Müller
410	Ulrich Müller
411	Ulrich Müller
412	Ulrich Müller
413	Ulrich Müller
414	Ulrich Müller
415	Ulrich Müller
416	Ulrich Müller
417	Ulrich Müller
418	Ulrich Müller
419	Ulrich Müller
420	Ulrich Müller
421	Ulrich Müller
422	Ulrich Müller
423	Ulrich Müller
424	Ulrich Müller
425	Ulrich Müller
426	Ulrich Müller
427	Ulrich Müller
428	Ulrich Müller
429	Ulrich Müller
430	Ulrich Müller
431	Ulrich Müller
432	Ulrich Müller
433	Ulrich Müller
434	Ulrich Müller
435	Ulrich Müller
436	Ulrich Müller
437	Ulrich Müller
438	Ulrich Müller
439	Ulrich Müller
440	Ulrich Müller
441	Ulrich Müller
442	Ulrich Müller
443	Ulrich Müller
444	Ulrich Müller
445	Ulrich Müller
446	Ulrich Müller
447	Ulrich Müller
448	Ulrich Müller
449	Ulrich Müller
450	Ulrich Müller
451	Ulrich Müller
452	Ulrich Müller
453	Ulrich Müller
454	Ulrich Müller
455	Ulrich Müller
456	Ulrich Müller
457	Ulrich Müller
458	Ulrich Müller
459	Ulrich Müller
460	Ulrich Müller
461	Ulrich Müller
462	Ulrich Müller
463	Ulrich Müller
464	Ulrich Müller
465	Ulrich Müller
466	Ulrich Müller
467	Ulrich Müller
468	Ulrich Müller
469	Ulrich Müller
470	Ulrich Müller
471	Ulrich Müller
472	Ulrich Müller
473	Ulrich Müller
474	Ulrich Müller
475	Ulrich Müller
476	Ulrich Müller
477	Ulrich Müller
478	Ulrich Müller
479	Ulrich Müller
480	Ulrich Müller
481	Ulrich Müller
482	Ulrich Müller
483	Ulrich Müller
484	Ulrich Müller
485	Ulrich Müller
486	Ulrich Müller
487	Ulrich Müller
488	Ulrich Müller
489	Ulrich Müller
490	Ulrich Müller
491	Ulrich Müller
492	Ulrich Müller
493	Ulrich Müller
494	Ulrich Müller
495	Ulrich Müller
496	Ulrich Müller
497	Ulrich Müller
498	Ulrich Müller
499	Ulrich Müller
500	Ulrich Müller

5 Unabhängige Fraktion Freie Bürger – Albert Grosse Subkollonik Eigenwinnung
UFFBASSE

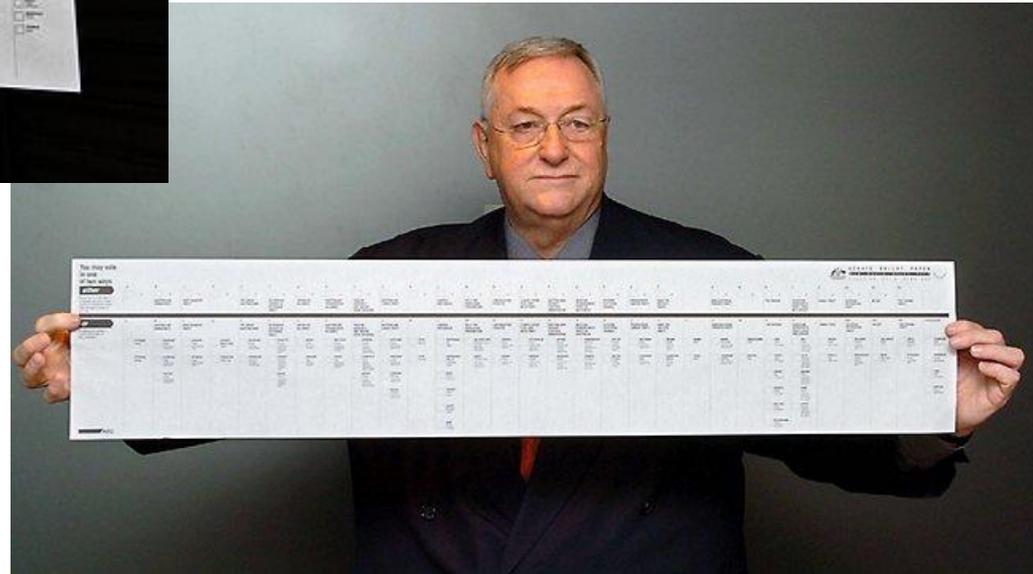
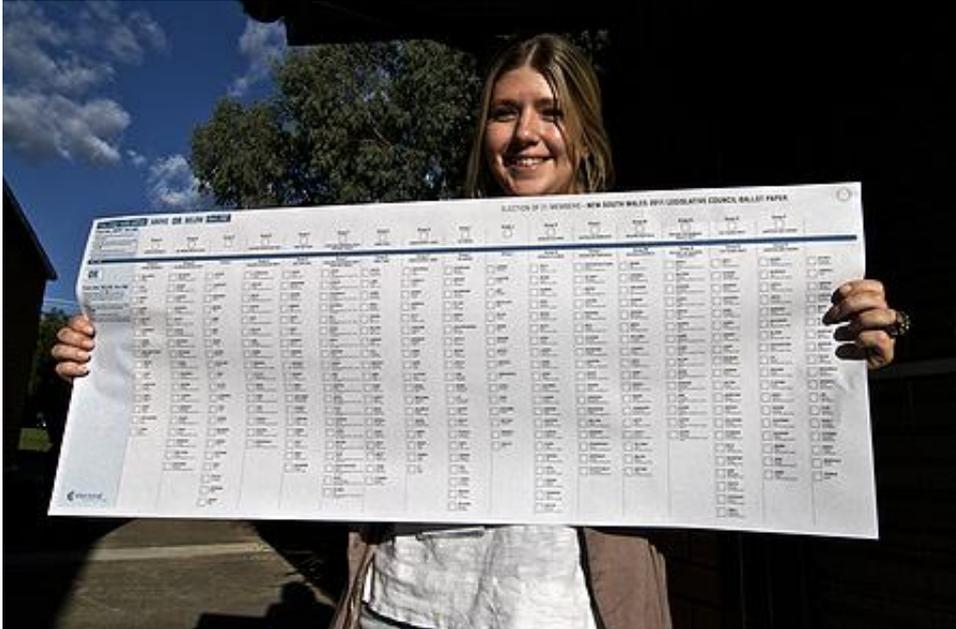
501	Ulrich Müller
502	Ulrich Müller
503	Ulrich Müller
504	Ulrich Müller
505	Ulrich Müller
506	Ulrich Müller
507	Ulrich Müller
508	Ulrich Müller
509	Ulrich Müller
510	Ulrich Müller
511	Ulrich Müller
512	Ulrich Müller
513	Ulrich Müller
514	Ulrich Müller
515	Ulrich Müller
516	Ulrich Müller
517	Ulrich Müller
518	Ulrich Müller
519	Ulrich Müller
520	Ulrich Müller
521	Ulrich Müller
522	Ulrich Müller
523	Ulrich Müller
524	Ulrich Müller
525	Ulrich Müller
526	Ulrich Müller
527	Ulrich Müller
528	Ulrich Müller
529	Ulrich Müller
530	Ulrich Müller
531	Ulrich Müller
532	Ulrich Müller
533	Ulrich Müller
534	Ulrich Müller
535	Ulrich Müller
536	Ulrich Müller
537	Ulrich Müller
538	Ulrich Müller
539	Ulrich Müller
540	Ulrich Müller
541	Ulrich Müller
542	Ulrich Müller
543	Ulrich Müller
544	Ulrich Müller
545	Ulrich Müller
546	Ulrich Müller
547	Ulrich Müller
548	Ulrich Müller
549	Ulrich Müller
550	Ulrich Müller
551	Ulrich Müller
552	Ulrich Müller
553	Ulrich Müller
554	Ulrich Müller
555	Ulrich Müller
556	Ulrich Müller
557	Ulrich Müller
558	Ulrich Müller
559	Ulrich Müller
560	Ulrich Müller
561	Ulrich Müller
562	Ulrich Müller
563	Ulrich Müller
564	Ulrich Müller
565	Ulrich Müller
566	Ulrich Müller
567	Ulrich Müller
568	Ulrich Müller
569	Ulrich Müller
570	Ulrich Müller
571	Ulrich Müller
572	Ulrich Müller
573	Ulrich Müller
574	Ulrich Müller
575	Ulrich Müller
576	Ulrich Müller
577	Ulrich Müller
578	Ulrich Müller
579	Ulrich Müller
580	Ulrich Müller
581	Ulrich Müller
582	Ulrich Müller
583	Ulrich Müller
584	Ulrich Müller
585	Ulrich Müller
586	Ulrich Müller
587	Ulrich Müller
588	Ulrich Müller
589	Ulrich Müller
590	Ulrich Müller
591	Ulrich Müller
592	Ulrich Müller
593	Ulrich Müller
594	Ulrich Müller
595	Ulrich Müller
596	Ulrich Müller
597	Ulrich Müller
598	Ulrich Müller
599	Ulrich Müller
600	Ulrich Müller

6 Die Linke
Die Linke

601	Ulrich Müller
602	Ulrich Müller
603	Ulrich Müller
604	Ulrich Müller
605	Ulrich Müller
606	Ulrich Müller
607	Ulrich Müller
608	Ulrich Müller
609	Ulrich Müller
610	Ulrich Müller
611	Ulrich Müller
612	Ulrich Müller
613	Ulrich Müller
614	Ulrich Müller
615	Ulrich Müller
616	Ulrich Müller
617	Ulrich Müller
618	Ulrich Müller
619	Ulrich Müller
620	Ulrich Müller
621	Ulrich Müller
622	Ulrich Müller
623	Ulrich Müller
624	Ulrich Müller
625	Ulrich Müller
626	Ulrich Müller
627	Ulrich Müller
628	Ulrich Müller
629	Ulrich Müller
630	Ulrich Müller
631	Ulrich Müller
632	Ulrich Müller
633	Ulrich Müller
634	Ulrich Müller
635	Ulrich Müller
636	Ulrich Müller
637	Ulrich Müller
638	Ulrich Müller
639	Ulrich Müller
640	Ulrich Müller
641	Ul

Complex ballot example 2

Australia



Related work

	This work		Groth 2005		Helios	
	P	V	P	V	P	V
Approval K-out-of-N	$2N [+ 3N]$	$4N [+ 5N]$	$6K + 4$	$3K + 3$	$6N + 2$	$8N + 4$
(0-N)-out-of-N	$4N [+ 3N]$	$8N [+ 5N]$	$2N + 4$	$N + 3$	$6N$	$8N$
$(K_{\min}-K_{\max})$ -out-of-N	$2(N + K_{\max}-K_{\min}) [+ 3N]$	$4(N + K_{\max}-K_{\min}) [+ 5N]$	-	-	$6N + 4(K_{\max}-K_{\min}) - 2$	$8N + 4(K_{\max}-K_{\min})$
Weighted (divisible) Vote = T shares	$2TN [+3N]$	$4TN [+5N]$	$10N + 4 *$	$5N + 2 *$	$(4T-2)(N+1)$	$4T(N+1)$
Rank K-out-of-N	$2N [+2KN +3N]$	$4N [+4KN +5N]$	$4N + 2 **$	$2N + 3 **$	$6(N+1)K + 2K$	$8(N+1)K + 4K$

* Does not support a limit per candidate.

** Ranks all candidates and limits the homomorphic tally to the Borba method.

Related work – continuation I

- Groth 2005
 - Complexity grows exponentially with the number of candidates and the number of votes allowed in the homomorphic tally.
 - Large number of candidates => large exponents size
 - Exponent size $\sim \log_2 (\#votes) * \# candidates$
 - Requires a crypto system with an easy decryption of $E(m_1+m_2, r_1+r_2) = E(m_1, r_1)E(m_2, r_2)$, e.g. Paillier.
 - Size of decryption table for 256 bits EC-ElGamal
10 candidates, 100 votes -> more than 25TB!!!

In practice, does not work for complex elections.

Related work – continuation II

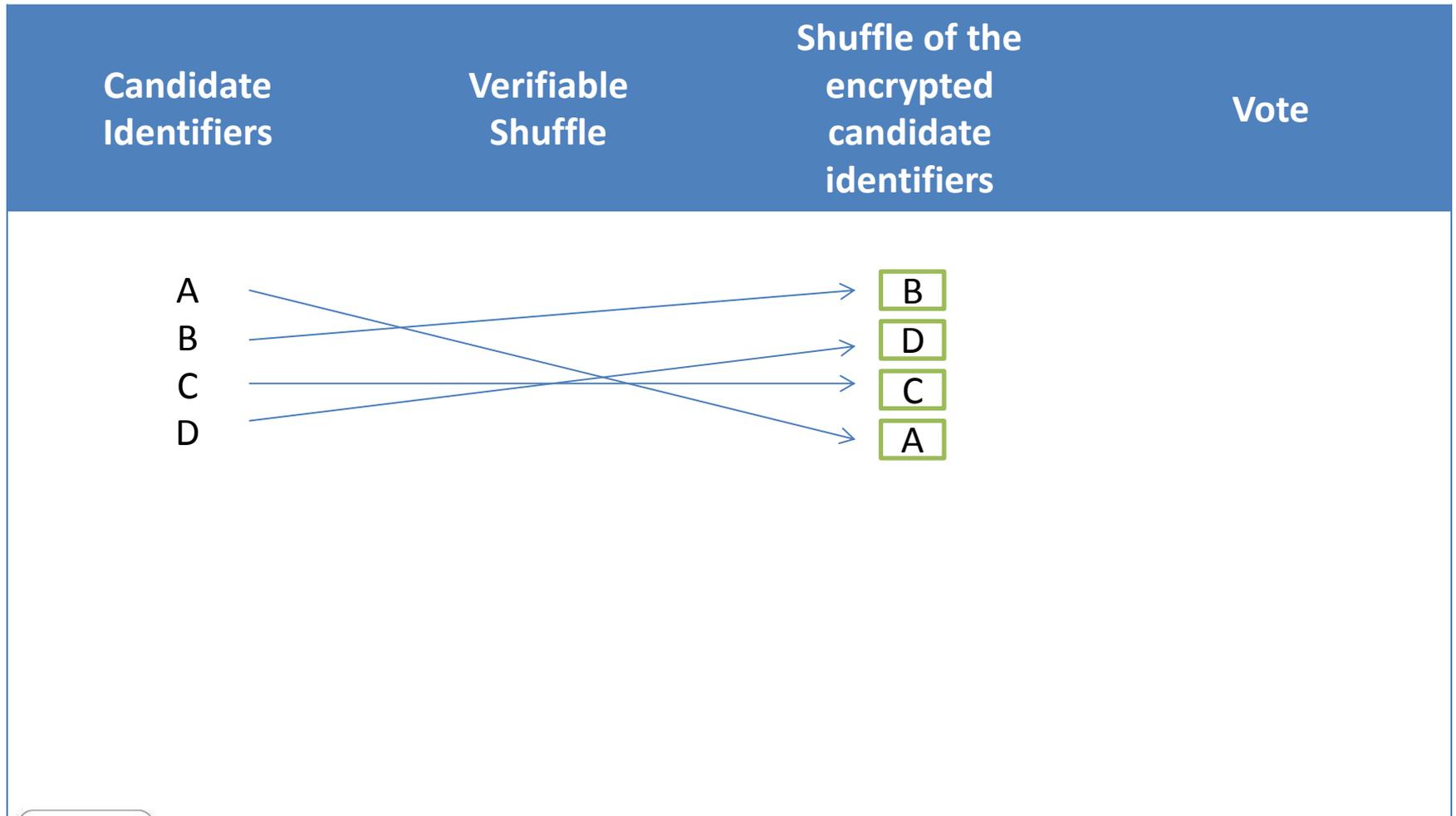
- Helios
 - Direct mix-net tallying is expensive because it involves one ciphertext per each possible option (candidate).
 - The number of ciphertexts can be reduced by using more expensive proofs.
 - No mix-net solution for ranked candidates.
 - Larger proofs.

A NEW WAY TO VERIFY AN ENCRYPTION OF A COMPLEX VOTE

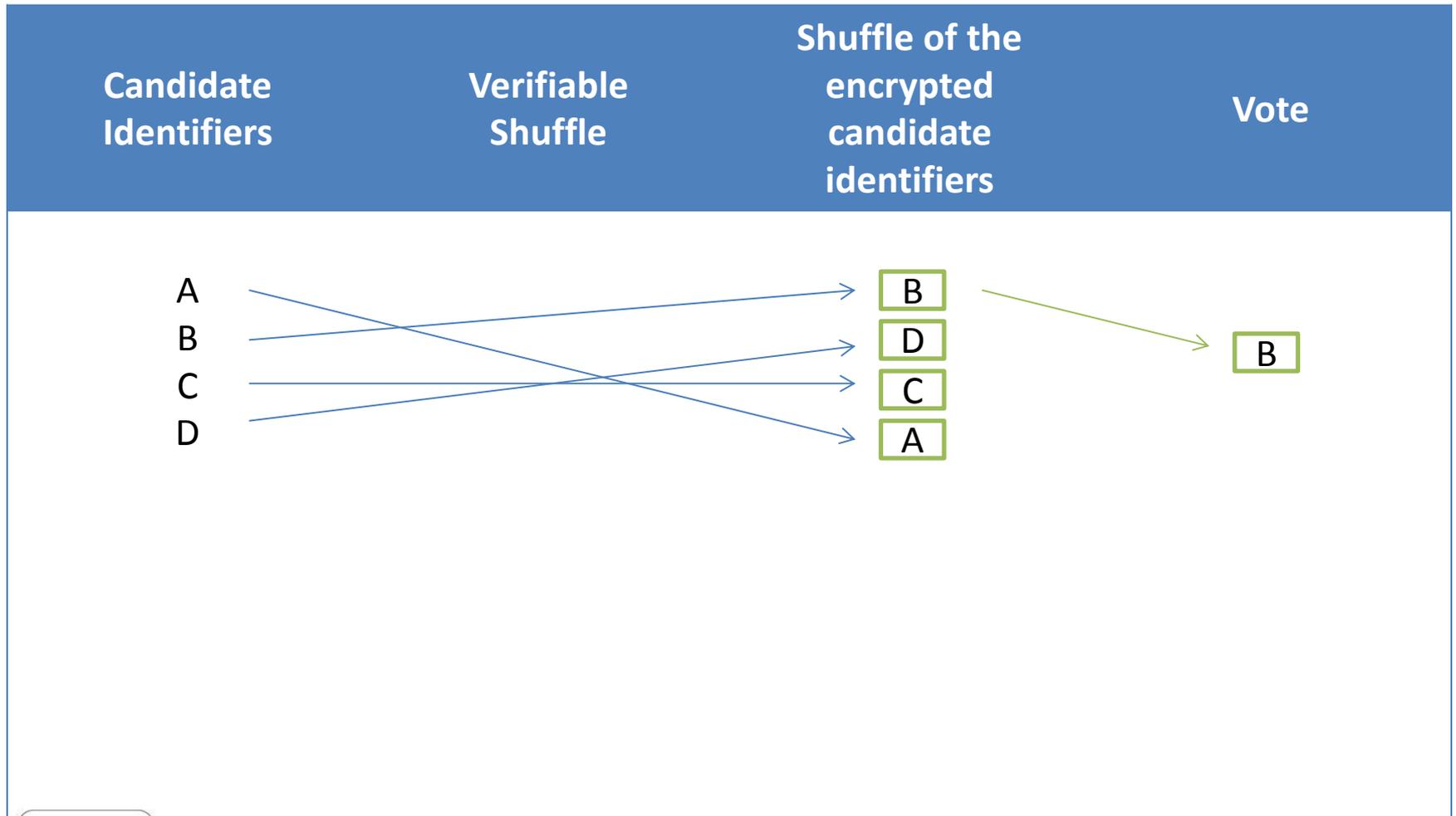
Key idea

1. Create a verifiable shuffle of a set of candidate identifiers.
 - Bayer and Groth 2012
2. Create the vote encryption directly from the shuffle output.
3. Add ZKPK to check ballot structure constrains.

Approval voting

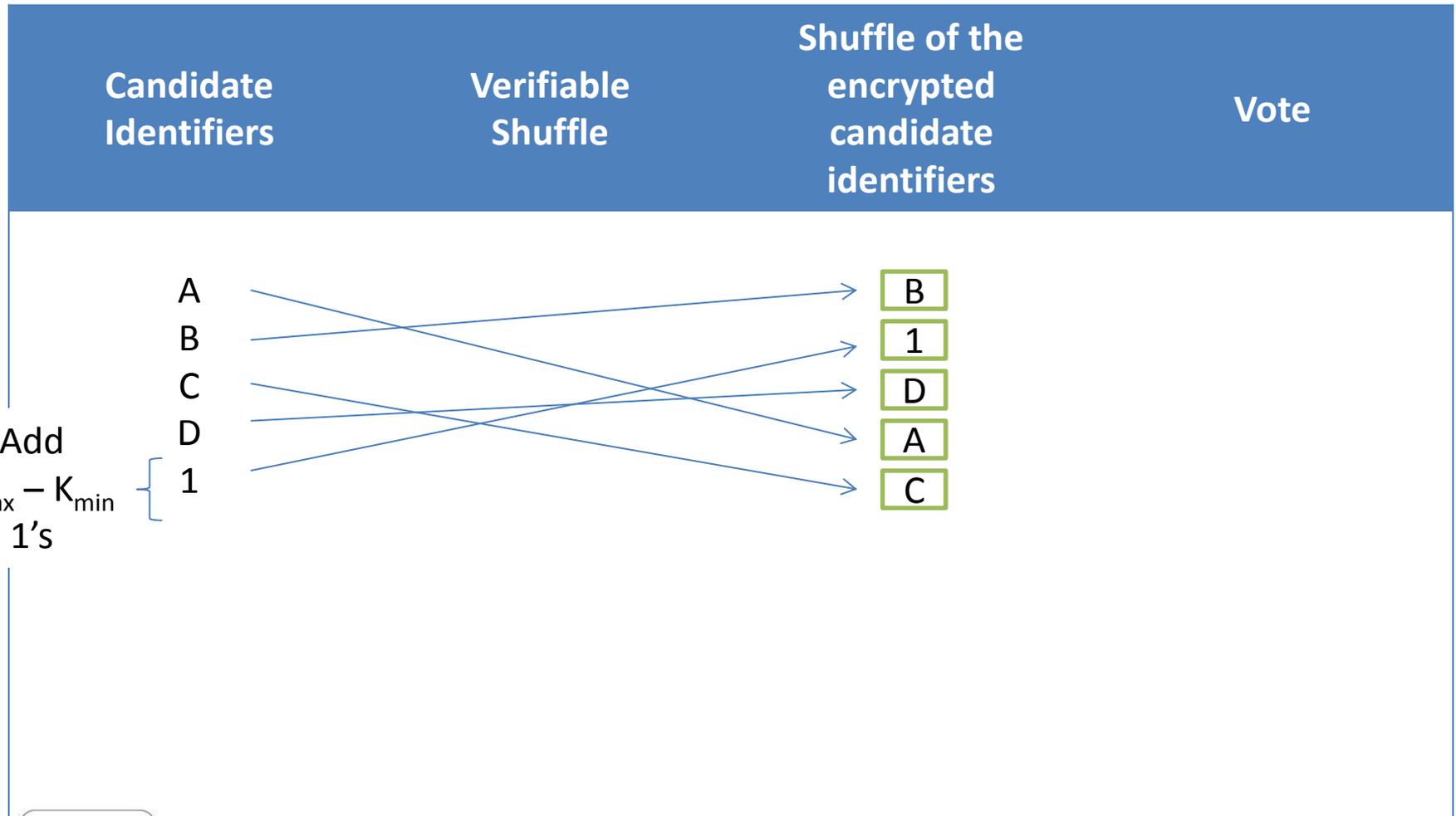


Approval voting



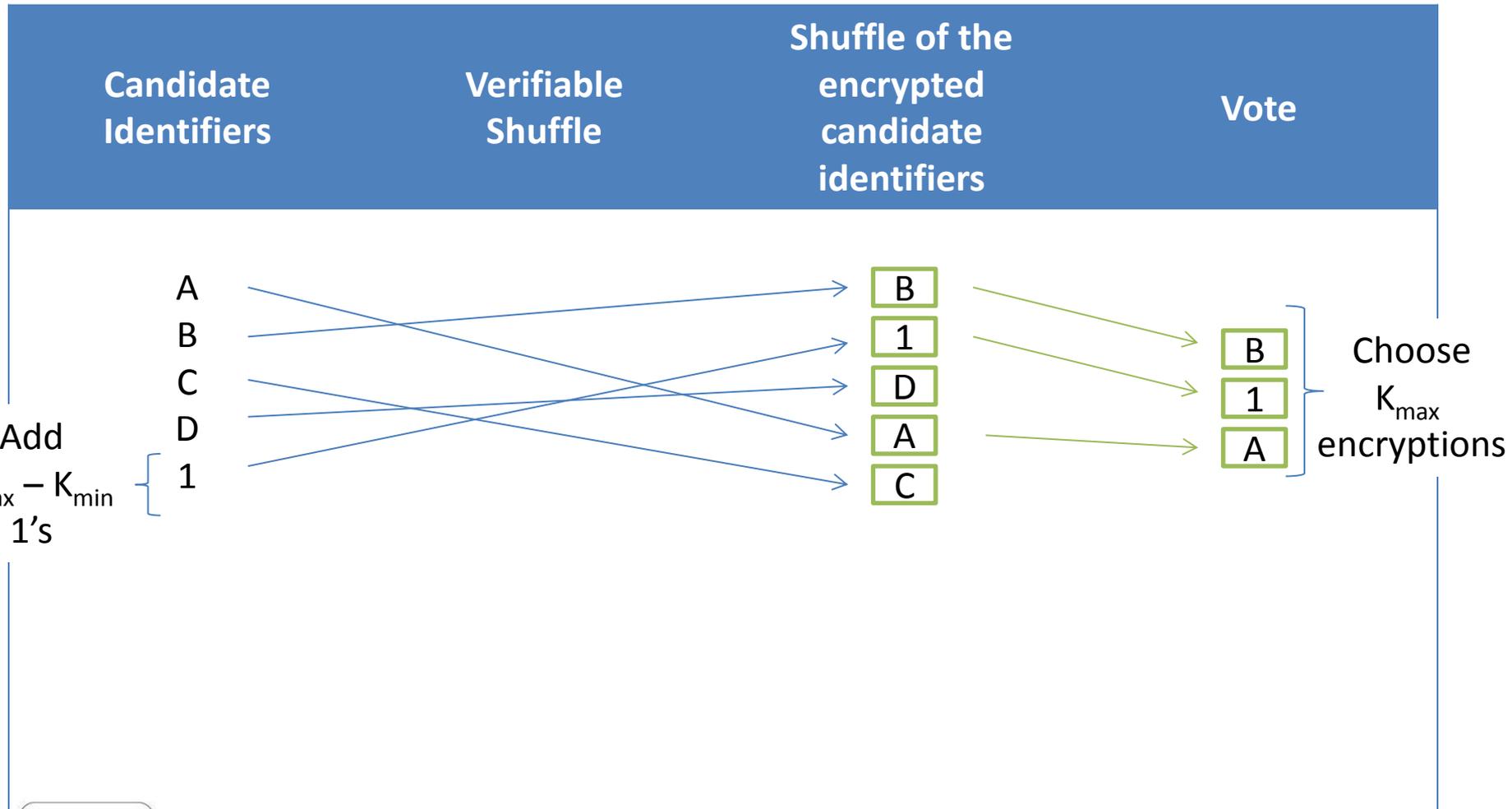
Approval voting $[K_{\min}, K_{\max}]$

Example : [2-3]

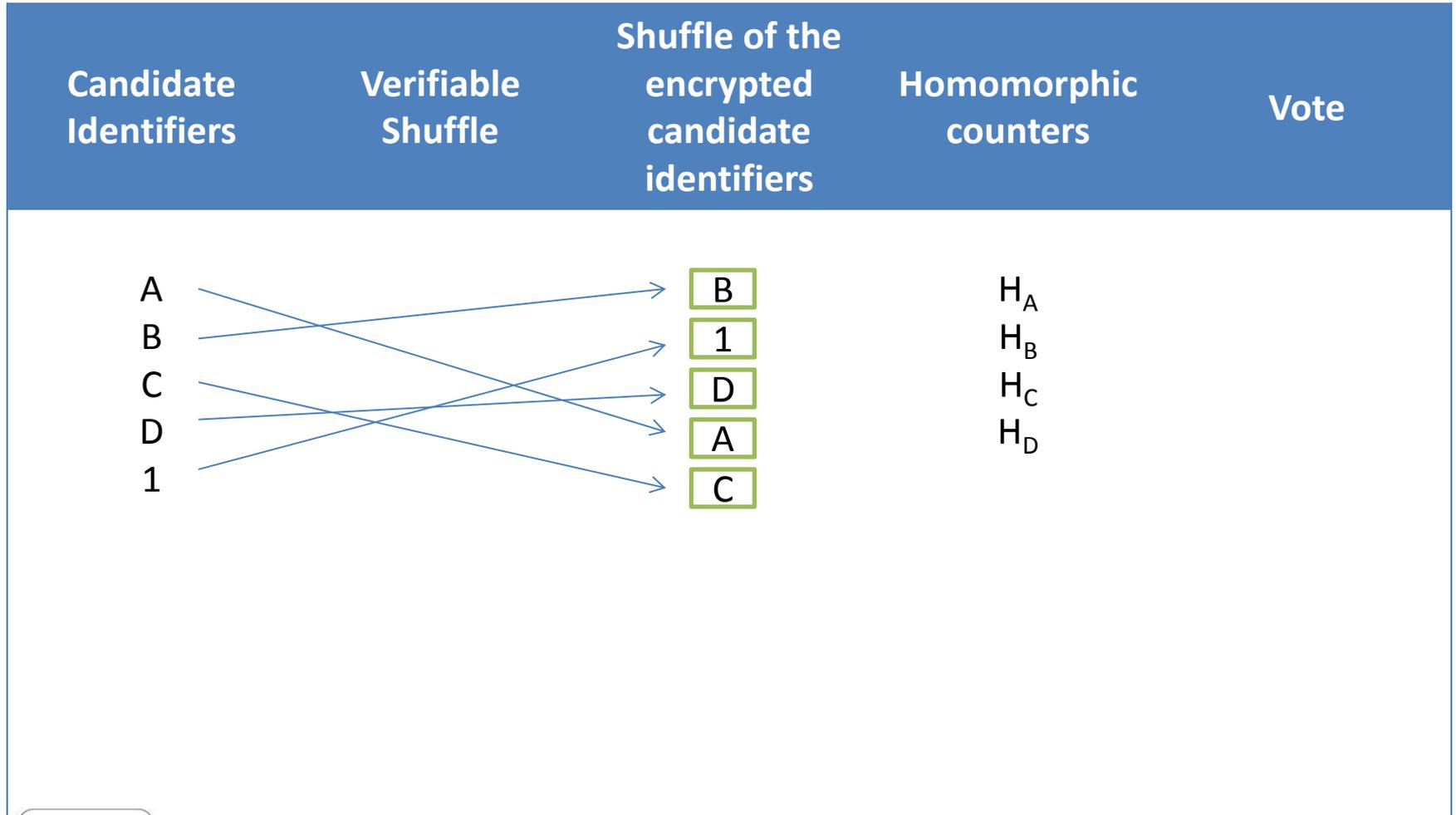


Approval voting $[K_{\min}, K_{\max}]$

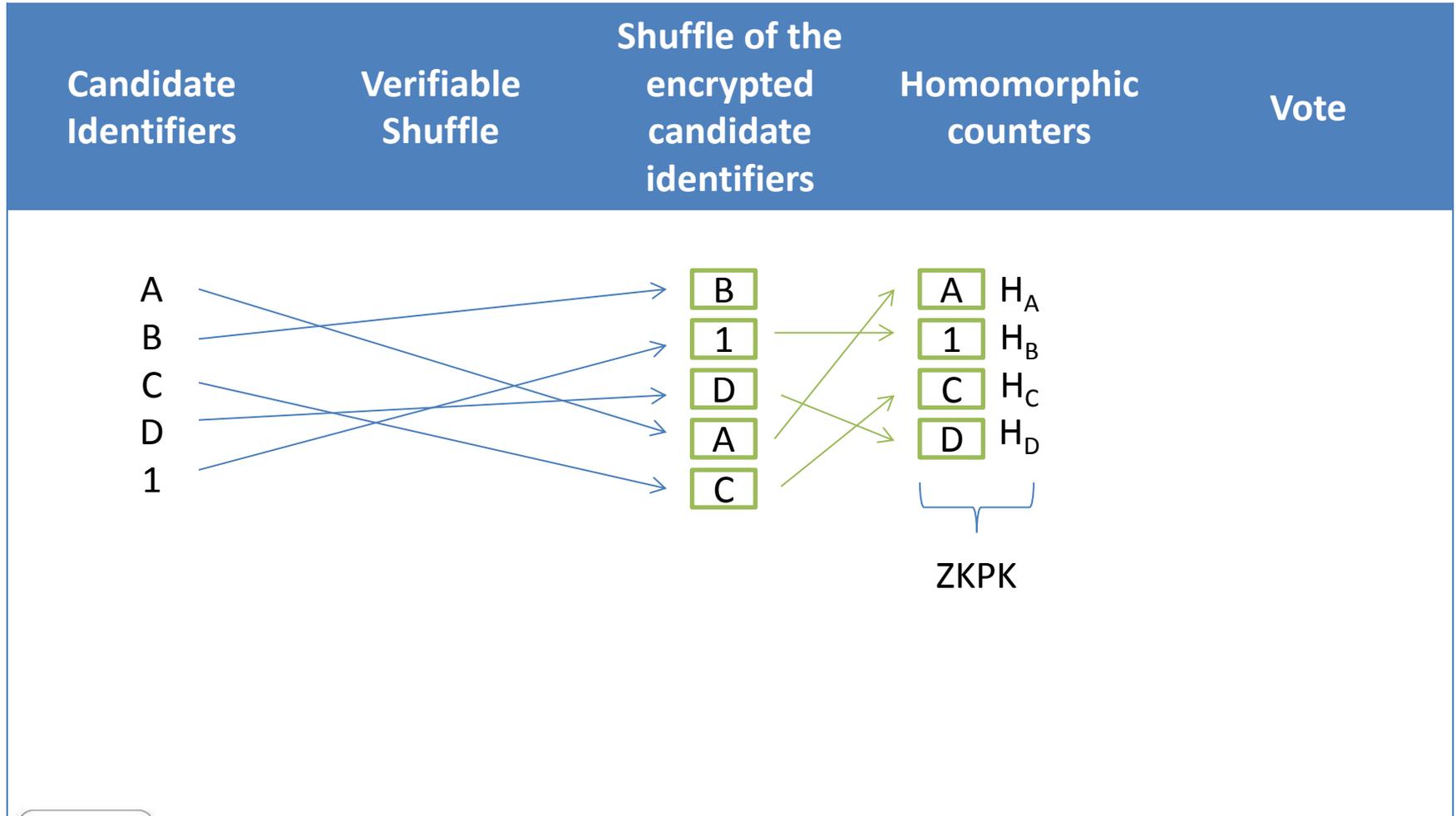
Example : $[2-3]$



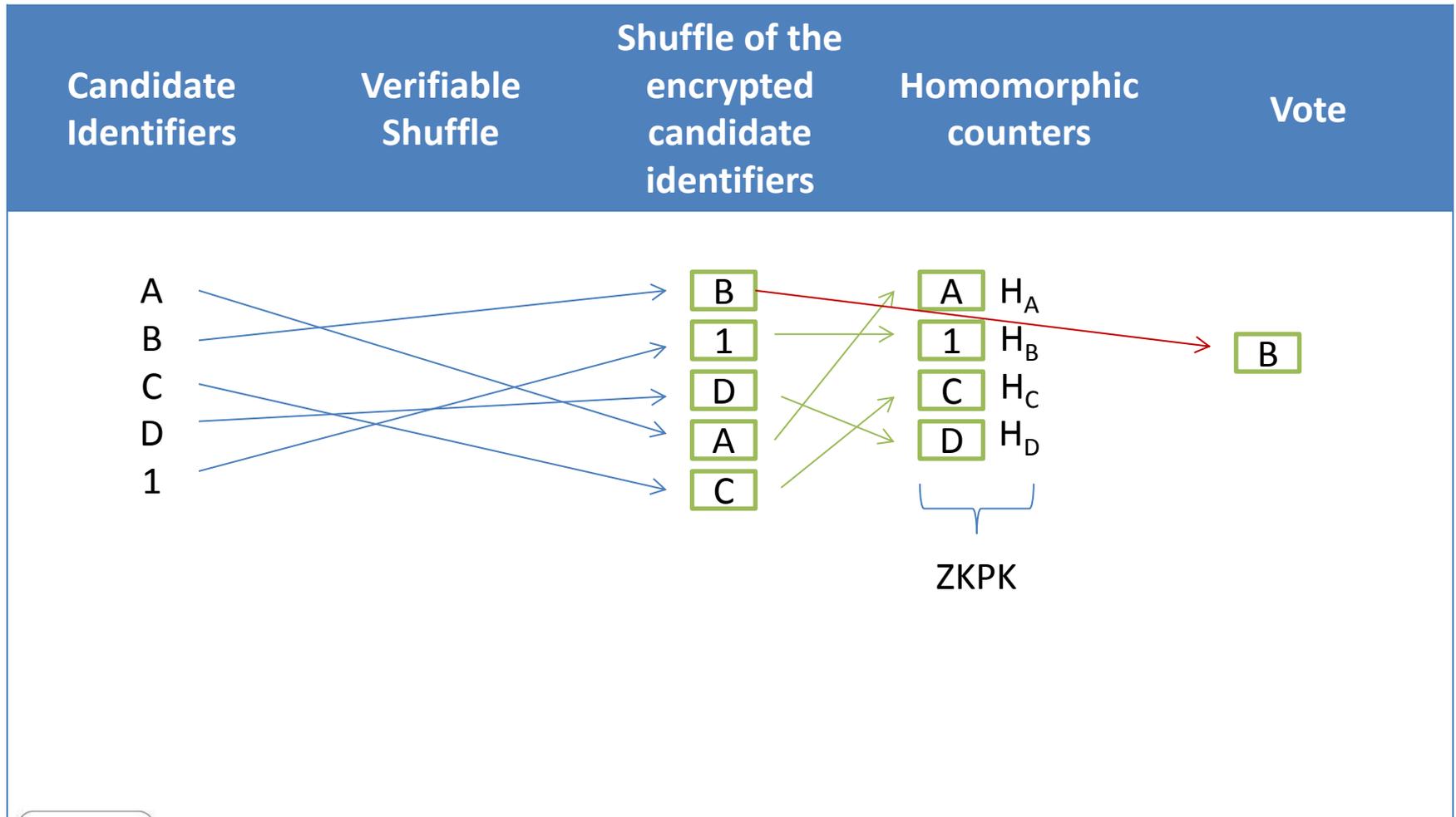
Approval voting with homomorphic tally



Approval voting with homomorphic tally



Approval voting with homomorphic tally



Ranked voting with homomorphic tally

Candidate
Identifiers

Homomorphic counters from N shuffles

A	1 H_{A1}	A H_{A2}	A H_{A3}	A H_{A4}
B	B H_{B1}	B H_{B2}	B H_{B3}	1 H_{B4}
C	C H_{C1}	1 H_{C2}	C H_{C3}	C H_{C4}
D	D H_{D1}	D H_{D2}	1 H_{D3}	D H_{D4}

1

Ranked voting with homomorphic tally

Candidate Identifiers

Homomorphic counters from N shuffles

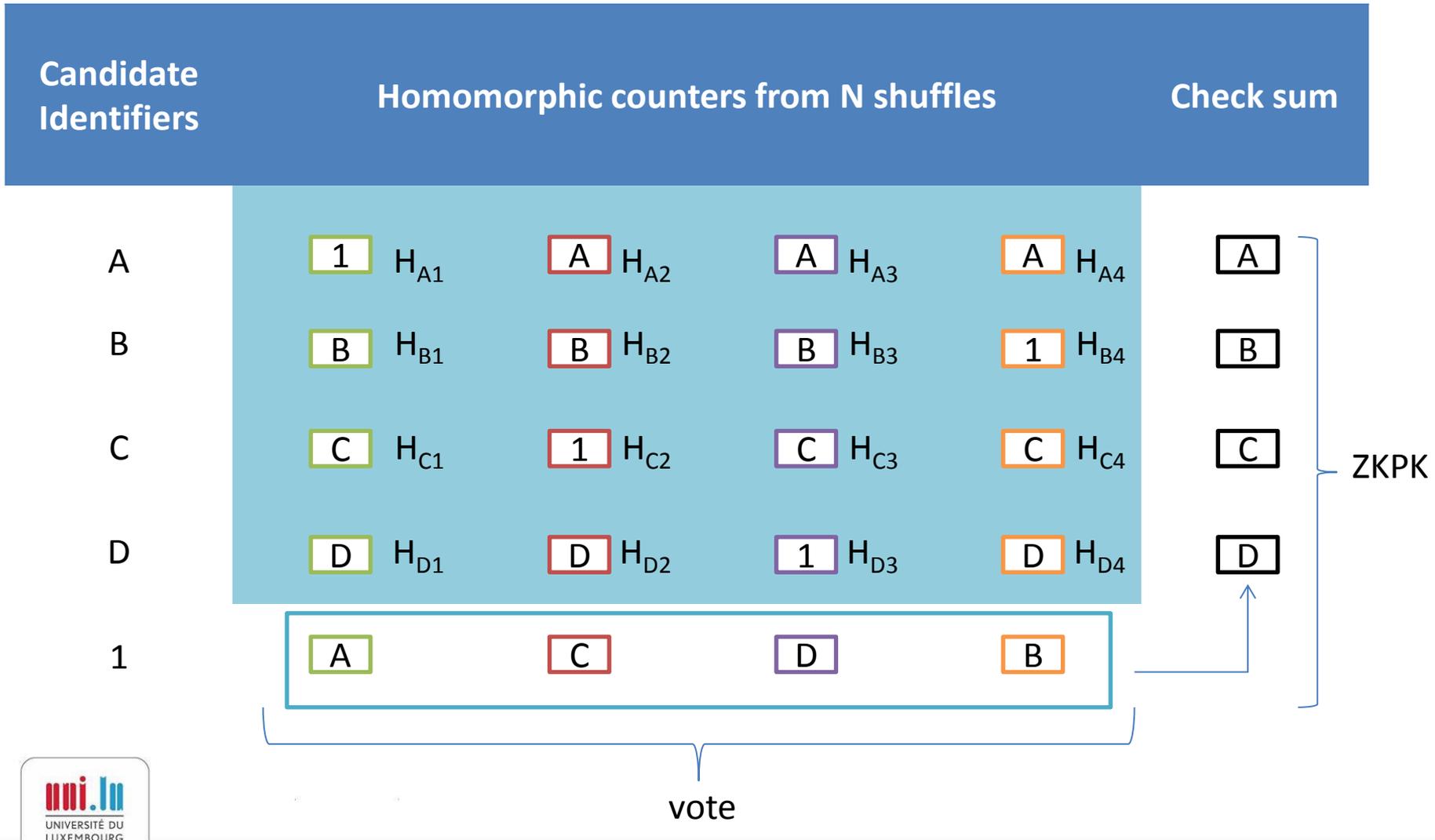
A	1 H_{A1}	A H_{A2}	A H_{A3}	A H_{A4}
B	B H_{B1}	B H_{B2}	B H_{B3}	1 H_{B4}
C	C H_{C1}	1 H_{C2}	C H_{C3}	C H_{C4}
D	D H_{D1}	D H_{D2}	1 H_{D3}	D H_{D4}

1

A C D B

vote

Ranked voting with homomorphic tally



A SINGLE VERIFICATION CODE FOR A COMPLEX BALLOT

Preliminaries

- Consider:
 - The usual ElGamal setup.
 - One independent generator (g_i) for every choice/candidate i .
 - Let $V = E(\prod_{l=1}^k g_{jl}, r_v)$ be the homomorphic product of the k ciphertexts that compose the vote.

The voter verification protocol (v1)

Vote Machine

Voter

$$S = \{s_1, \dots, s_k\}$$



$$V = E(\prod_{l=1}^k g_{sl}, r_v)$$

$$w_1, \dots, w_N, r \xleftarrow{R} \mathbb{Z}_q$$

$$W = E(\prod_{i=1}^N g_i^{w_i}, r)$$

$$\sigma = \prod_{l=1}^k g_l^{w_l}$$

$$\sigma, V, W$$



$$V, W$$



The voter verification protocol (v1)

Vote Machine

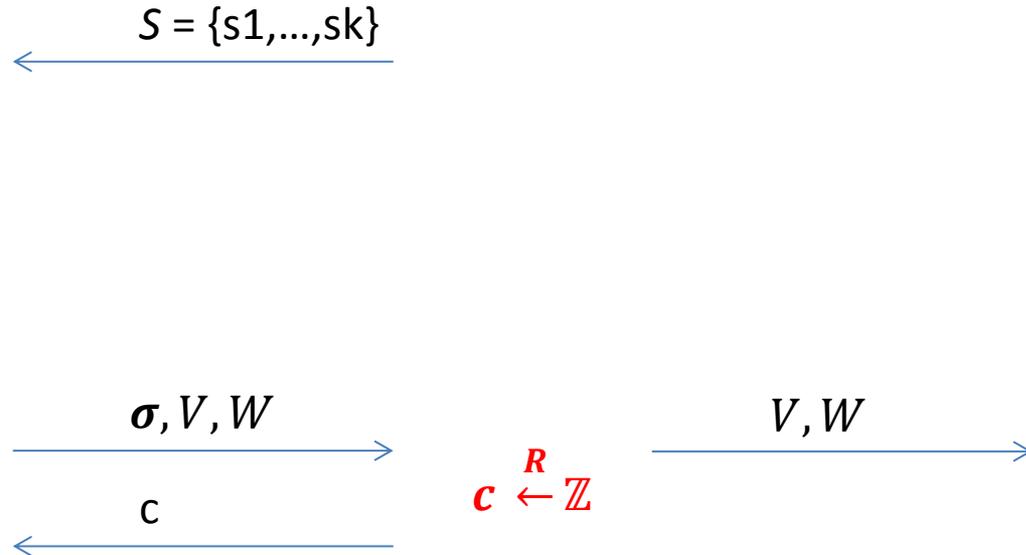
Voter

$$V = E(\prod_{l=1}^k g_{sl}, r_v)$$

$$w_1, \dots, w_N, r \stackrel{R}{\leftarrow} \mathbb{Z}_q$$

$$W = E(\prod_{i=1}^N g_i^{w_i}, r)$$

$$\sigma = \prod_{l=1}^k g_l^{w_k}$$



The voter verification protocol (v1)

Vote Machine
Voter

$$S = \{s_1, \dots, s_k\}$$

$$V = E(\prod_{l=1}^k g_{sl}, r_v)$$

$$w_1, \dots, w_N, r \xleftarrow{R} \mathbb{Z}_q$$

$$W = E(\prod_{i=1}^N g_i^{w_i}, r)$$

$$\sigma = \prod_{l=1}^k g_l^{w_l}$$

$$\sigma, V, W$$

$$V, W$$

$$c$$

$$c \xleftarrow{R} \mathbb{Z}$$

$$\forall s_i \in S: r_{si} = w_{si} + c$$

$$\forall l \notin S: r_l = w_l$$

$$P_r = \text{ZKPK}[W \otimes V^c = E(\prod_{i=1}^N g_i^{r_i}, r')]$$

$$r_1, \dots, r_n, P_r$$

$$c, r_1, \dots, r_n, P_r$$

$$\sigma ? = \prod_{si \in S} g_{si}^{r_{si} - c}$$

 P_r !?

The voter verification protocol (v1)

Vote Machine
Voter

$$S = \{s_1, \dots, s_k\}$$

$$V = E(\prod_{l=1}^k g_{sl}, r_v)$$

$$w_1, \dots, w_N, r \xleftarrow{R} \mathbb{Z}_q$$

$$W = E(\prod_{i=1}^N g_i^{w_i}, r)$$

$$\sigma = \prod_{l=1}^k g_l^{w_l}$$

$$\sigma, V, W$$

$$V, W$$

$$c$$

$$c \xleftarrow{R} \mathbb{Z}$$

$$\forall s_i \in S: r_{s_i} = w_{s_i} + c$$

$$\forall l \notin S: r_l = w_l$$

$$P_r = \text{ZKPK}[W \otimes V^c = E(\prod_{i=1}^N g_i^{r_i}, r')]$$

$$r_1, \dots, r_n, P_r$$

$$c, r_1, \dots, r_n, P_r$$

 P_r !?

$$\sigma ? = \prod_{s_i \in S} g_{s_i}^{r_{s_i} - c}$$

The voter verification protocol (v1)

Vote Machine
Voter

$$S = \{s_1, \dots, s_k\}$$

$$V = E(\prod_{l=1}^k g_{sl}, r_v)$$

$$w_1, \dots, w_N, r \xleftarrow{R} \mathbb{Z}_q$$

$$W = E(\prod_{i=1}^N g_i^{w_i}, r)$$

$$\sigma = \prod_{l=1}^k g_l^{w_l}$$

$$\sigma, V, W$$

$$c$$

$$c \xleftarrow{R} \mathbb{Z}$$

$$V, W$$

$$\forall s_i \in S: r_{s_i} = w_{s_i} + c$$

$$\forall l \notin S: r_l = w_l$$

$$P_r = \text{ZKPK}[W \otimes V^c = E(\prod_{i=1}^N g_i^{r_i}, r')]$$

$$r_1, \dots, r_n, P_r$$

$$c, r_1, \dots, r_n, P_r$$

 P_r !?

$$\sigma ? = \prod_{s_i \in S} g_{s_i}^{r_{s_i} - c}$$

UNIVERSAL A VERIFICATION CODE

The voter verification protocol (v2)

Vote Machine

Voter

$$S = \{s_1, \dots, s_k\}$$



$$V = E(v, r_v)$$

$$\sigma \stackrel{R}{\leftarrow} G_q, r \stackrel{R}{\leftarrow} \mathbb{Z}_q$$

$$W = E(\sigma, r)$$

$$\sigma, V, W$$



$$V, W$$



The voter verification protocol (v2)

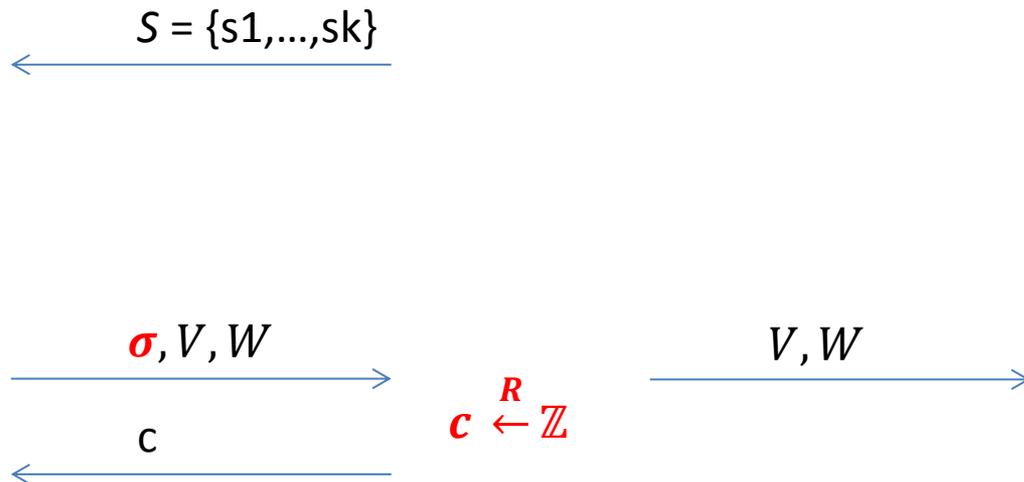
Vote Machine

Voter

$$V = E(v, r_v)$$

$$\sigma \xleftarrow{R} G_q, r \xleftarrow{R} \mathbb{Z}_q$$

$$W = E(\sigma, r)$$



The voter verification protocol (v2)

Vote Machine

Voter

$$S = \{s_1, \dots, s_k\}$$

$$V = E(v, r_v)$$

$$\sigma \xleftarrow{R} G_q, r \xleftarrow{R} \mathbb{Z}_q$$

$$W = E(\sigma, r)$$

$$\sigma, V, W$$

$$V, W$$

$$c$$

$$c \xleftarrow{R} \mathbb{Z}$$

$$P_r = \text{ZKPK}[W \otimes V^c = E(\theta, r')]$$

$$\theta, P_r$$

$$\theta, c, P_r$$

$$\sigma ? = \theta / v^c$$

$$P_r !?$$

The voter verification protocol (v2)

Vote Machine

$$V = E(v, r_v)$$

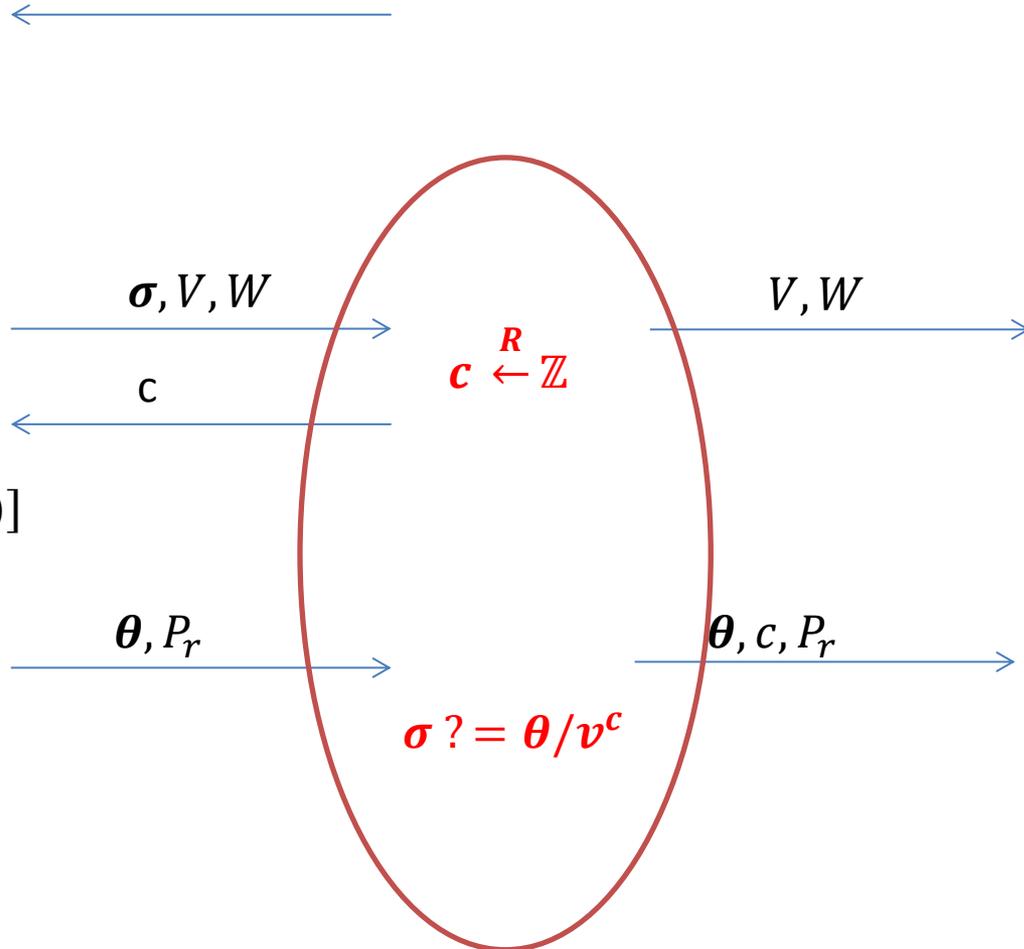
$$\sigma \xleftarrow{R} G_q, r \xleftarrow{R} \mathbb{Z}_q$$

$$W = E(\sigma, r)$$

$$P_r = \text{ZKPK}[W \otimes V^c = E(\theta, r')]$$

Voter

$$S = \{s_1, \dots, s_k\}$$



The voter verification protocol (v2)

Vote Machine

Voter

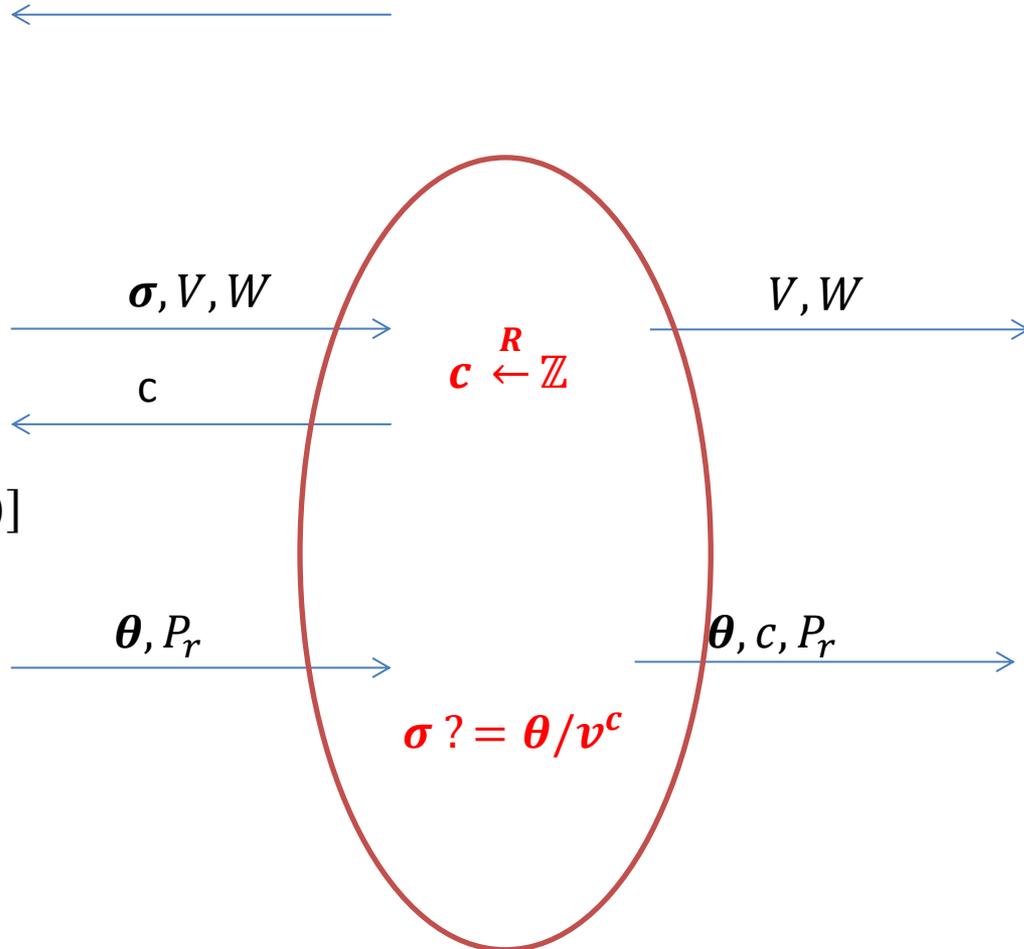
$$S = \{s_1, \dots, s_k\}$$

$$V = E(v, r_v)$$

$$\sigma \xleftarrow{R} G_q, r \xleftarrow{R} \mathbb{Z}_q$$

$$W = E(\sigma, r)$$

$$P_r = \text{ZKPK}[W \otimes V^c = E(\theta, r')]$$



$P_r!$?

The voter verification protocol (v2)

Vote Machine

$$V = E(v, r_v)$$

$$\sigma \stackrel{R}{\leftarrow} G_q, r \stackrel{R}{\leftarrow} \mathbb{Z}_q$$

$$W = E(\sigma, r)$$

$$P_r = \text{ZKPK}[W \otimes V^c = E(\theta, r')]$$

Voter

$$S = \{s_1, \dots, s_k\}$$

$$\sigma, V, W$$

$$c$$

$$\theta, P_r$$

$$c \stackrel{R}{\leftarrow} \mathbb{Z}$$

$$\sigma ? = \theta / v^c$$

$$V, W$$

$$\theta, c, P_r$$

$$P_r!?$$

Thank you!

Questions?