Practical Construction for Secure Trick-Taking Games Even With Cards Set Aside

Rohann Bella[1], Xavier Bultel[1], Céline Chevalier[2], Pascal Lafourcade[3], **Charles Olivier-Anclin**[3,4]

Journées C2 2023

1 - INSA Centre Val de Loire, LIFO, France

2 - CRED, Université Paris-Panthéon-Assas and DIENS, École normale supérieure

3 - Université Clermont-Auvergne, LIMOS

4 - be ys Pay

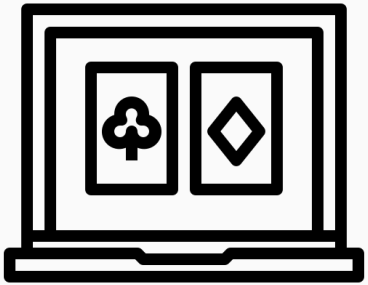
No cards set aside

Spades, Whist, Belote, Coinche, Bridge

Cards set aside

Tarot, Skate

Online Trick-Tacking Games



- For fun
- Online casino

Cheater in Online Casino

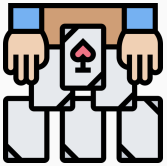
- Real money 
- Reputation loss 
- Less trust 

Trust Model

Weak: Trusted server

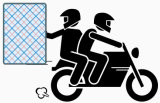
Stronger: No trusted server

Preventing Frauds



Unpredictability

Cheating-resistance



Theft-resistance

Hand-privacy

Game-privacy

Cards Set Aside

Expectations

Cards set aside behave like any player's hand.

Dog's Security:

Original Idea from FC'19

Xavier Bultel and Pascal Lafourcade. *"Secure trick-taking game protocols - how to play online spades with cheaters"*. In FC 19.

FC'19

- Too specific 
- Slow shuffle



≈ 20 seconds

Our New Protocols

- Generic 
- Games with cards set aside 
- Efficient shuffle



≈ 1 second

Building Block: ElGamal Encryption

Encryption & Decryption:

KeyGen($\mathfrak{K}$): $\mathsf{sk} \xleftarrow{\$} \mathbb{Z}_p^*$, $\mathsf{pk} = g^{\mathsf{sk}}$.

Returns $(\mathsf{pk}, \mathsf{sk})$

Enc(m, pk): $y \xleftarrow{\$} \mathbb{Z}_p^*$.

Returns $c = (g^y, m \cdot \mathsf{pk}^y)$

Dec(c, sk): $c = (c_1, c_2)$.

Returns $m = c_2 \cdot c_1^{-\mathsf{sk}}$

Randomisation:

Rand(c, r, pk): Computes $c_1' = c_1 \cdot g^r$ and $c_2' = c_2 \cdot \mathsf{pk}^r$.

Returns $c' = (c_1', c_2')$.

Building Block: Non-Interactive Zero-Knowledge Proofs

- Setup($\mathcal{L}$) $\rightarrow$ params.
- ZK(ϕ, w) $\rightarrow \pi$ that $\phi \in \mathcal{L}$.
- Ver(ϕ, π) $\rightarrow$ 0 or 1.

A NIZK proof requires the following properties:

Completeness	Soundness	Zero-Knowledge
$\text{Ver}(\phi, \text{ZK}(\phi)) = 1$.	There exists an extractor Ext.	There exists a simulator Sim.

Card and Hand Representation

$$\mathsf{id} = (\mathsf{suit}, \mathsf{val})$$

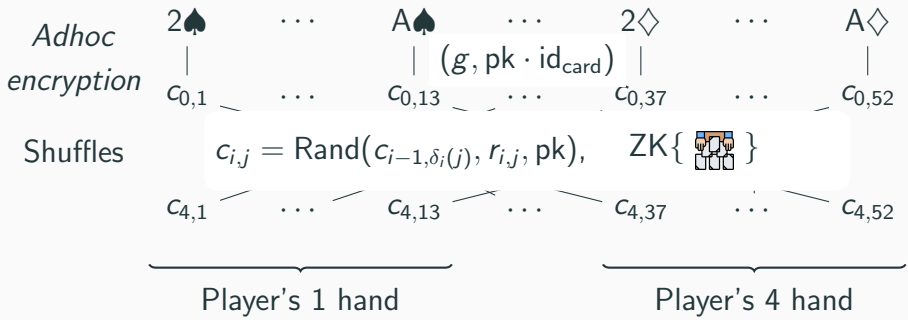
$$\{c_i\}_{i\in[\![1,52]\!]} \xleftarrow{\mathsf{Enc}_{\mathsf{ek}}(\cdot)} \{\mathsf{id}_i\}_{i\in[\![1,52]\!]}$$

$$\{\mathsf{id}_i\}_{i\in[\![1,13]\!]} \xleftarrow{\mathsf{Dec}_{\mathsf{dk}}(\cdot)} \{c_i^*\}_{i\in[\![1,13]\!]}$$

Card Dealing - Shuffle

id: cards, $r_{i,j}$: random numbers, $\delta_i(j)$ permutations.

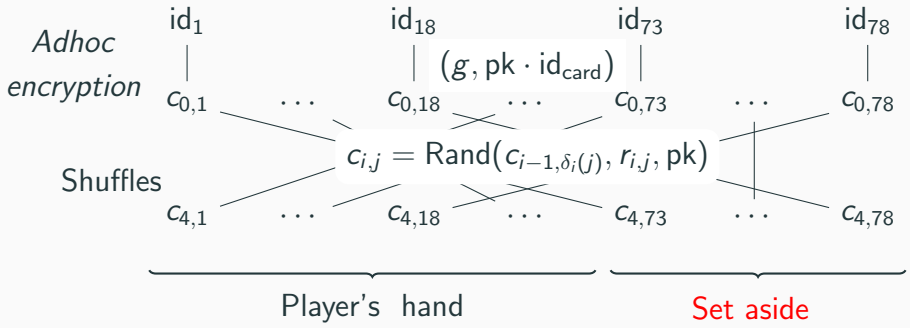
$$\mathsf{pk} = \prod_{i=1}^{4} \mathsf{pk}_i$$



The Case of Tarot

id: cards, $r_{i,j}$: random numbers, $\delta_i(j)$ permutations.

$$\mathsf{pk} = \prod_{i=1}^{4} \mathsf{pk}_i$$



Card Dealing: Recovery

One ciphertext encrypting a card:

$$c = (c_1 = g^{r_1+r_2+r_3+r_4}, c_2 = \mathsf{id}_j \cdot \mathsf{pk}^{r_1+r_2+r_3+r_4}) \qquad \text{for } \mathsf{pk} = \prod_{i=1}^{4} \mathsf{pk}_i$$


sk_2


sk_3


sk_4

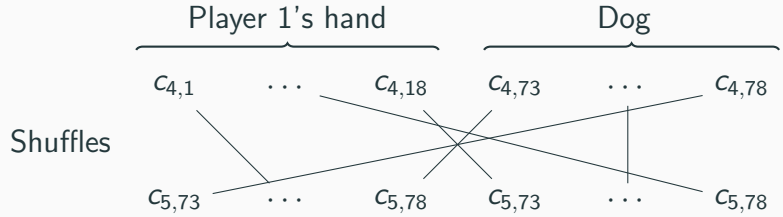
produces $\theta_i = c_1^{\mathsf{sk}_i}$.


Player 1

uses the values $c^* \leftarrow \left(c_1, \frac{c_2}{\theta_2 \cdot \theta_3 \cdot \theta_4}\right)$,

and recovers its card  $\leftarrow \mathsf{Dec}_{\mathsf{sk}_1}(c^*)$

Producing the Cards Set Aside

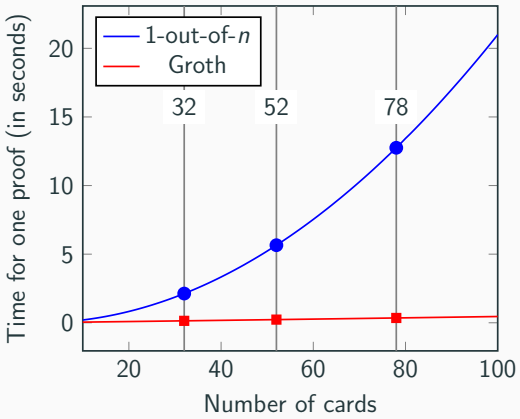


Dog's security:

For A the set of authorised card in the dog.

$$\mathsf{ZK}\left\{\mathsf{sk}_i : \bigwedge_{[\![73,78]\!]} \bigvee_{\mathsf{A}} \mathsf{id}_l = \mathsf{Dec}_{\mathsf{sk}}(c)\right\},$$

Efficiency of the Proof of Shuffle



→ Multiple Schnorr proofs.

→ Groth proof of shuffle [Gro10].

Game Phase

Playing, a card id

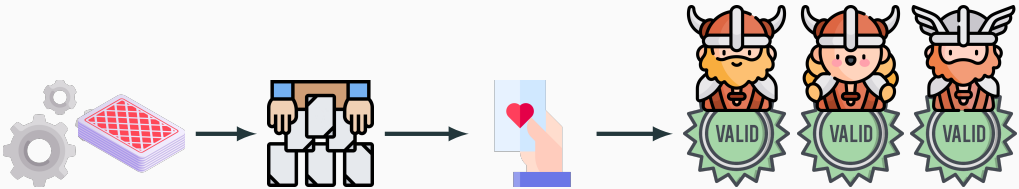
- Prove ownership of the cards: $\Pi_0 = \mathrm{ZK}\{\mathsf{sk} : \mathsf{id} = \mathrm{Dec}_{\mathsf{sk}}(c_t^*)\}$.
- Prove that the play follows the rules (not possible with real cards).

$$\Pi_1 = \mathrm{ZK}\left\{\mathsf{sk} : \bigwedge_{\substack{j \in [\![13\cdot(n-1)+1, 13\cdot n]\!] \\ j \notin U_n \cup \{t\}}} \bigvee_{l \in L} \mathsf{id}_l = \mathrm{Dec}_{\mathsf{sk}}(c_j^*)\right\}$$

Verifying

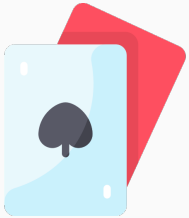
Benchmark

	FC'19		**Ours**	
	Prove	Verify	Prove	Verify
Shuffle	5.65 s	5.72 s	235 ms	176 ms
Play	105 ms		105 ms	



52 ≈ 10 seconds

Merci !



eprint.iacr.org/2023/309