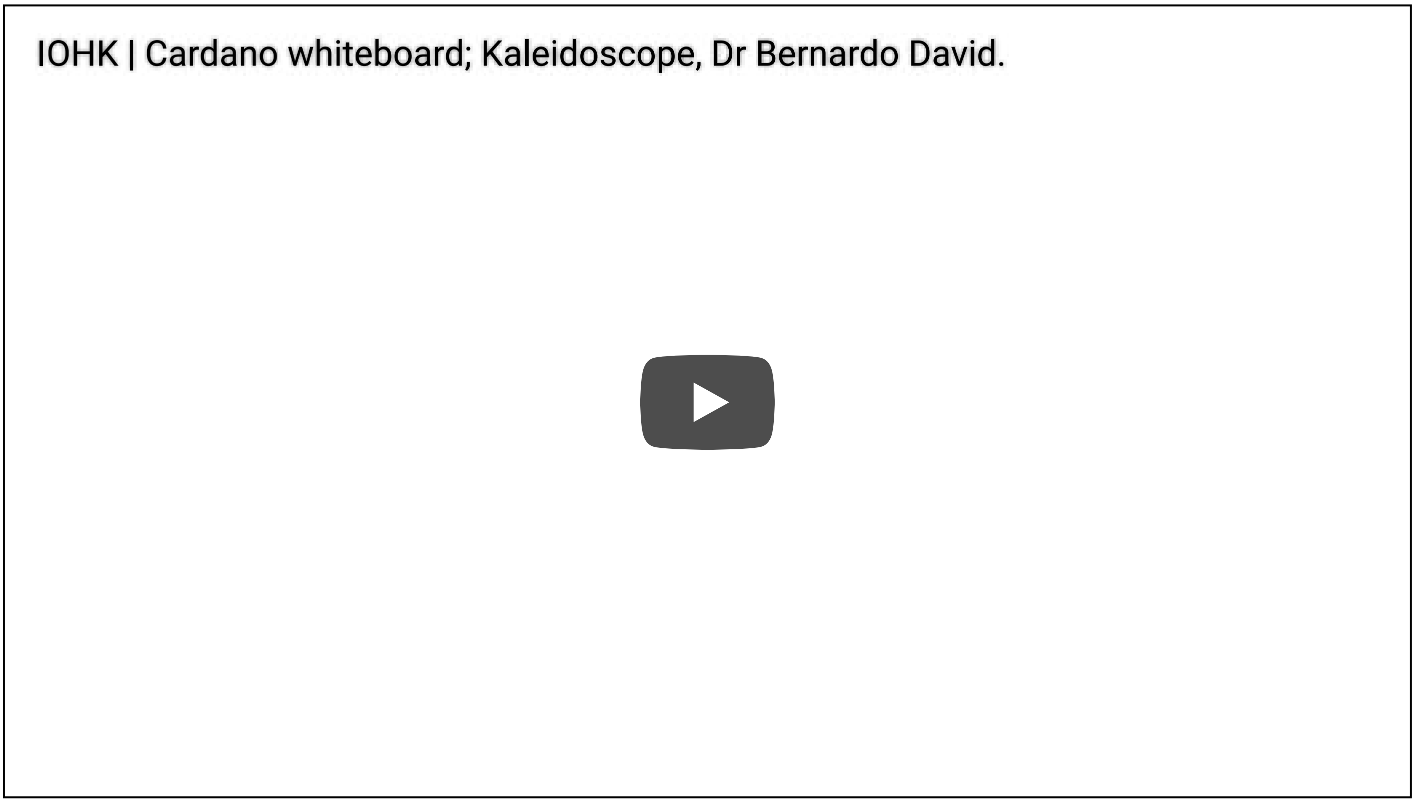
INPUT | OUTPUT

IOHK | BLOG

Kaleidoscope – a cryptographic protocol for securely playing poker

Bernardo David presents the research paper at Financial Cryptography 2018

MARCH 01, 2018 BERNARDO DAVID 8 MIN READ


IOHK | Cardano whiteboard; Kaleidoscope, Dr Bernardo David.

Poker is arguably one of the most popular card games in the world, both in casinos and on the internet. Online poker has become increasingly popular after a boom in the early 2000s, fueling a growing market with revenues estimated in the tens of billions of dollars. However, the current model of online gambling forces users to blindly trust the online casinos, who could easily rig games or suffer attacks from disgruntled employees who aim to make easy money. In fact, this state of affairs not only represents a threat but has resulted in real-world attacks.

A clear alternative to using online casinos consists of using cryptographic protocols for securely playing poker over a network without trusting any third party. In fact, constructing such protocols has been a research topic since the early days of modern cryptography. Shamir, Rivest and Adleman proposed the first candidate protocol to this end only a few years after publishing the famous RSA public key encryption scheme. Their seminal effort initiated a long line of research that has produced countless results over the years. However, no cryptographic poker protocol has ever been adopted for real applications, mainly due to the following issues:

1 - Security: The security guarantees of existing poker protocols are not clearly defined, so it is hard to understand the level of security that these protocols actually provide and how reliable they are.

2 - Efficiency: Most of the existing poker protocols rely on costly cryptographic techniques that incur high computational and communication overheads, which in the real world result in boring games with long delays.

3 - Financial considerations: Previous poker protocols could not ensure that winners received their financial rewards, even though classic cryptographic techniques could ensure that a game of poker was played honestly (i.e. without allowing players to cheat or learn each other's private data).

IOHK | Research; Kaleidoscope & Royale, Dr Mario Larangeira.

In a recent paper to be presented at the Financial Cryptography 2018 conference, we construct Kaleidoscope, the first cryptographic poker protocol to address all three issues above. Kaleidoscope is the first protocol to be proven secure according to a comprehensive security model that formally and clearly captures all the properties and guarantees commonly required from a poker protocol. Moreover, Kaleidoscope employs blockchain techniques to ensure that winners receive their rewards and that cheaters are financially penalized. Even though it is mathematically proven to achieve security while providing financial rewards and penalty enforcements, Kaleidoscope achieves very high efficiency in comparison to existing solutions (which have not been formally proven secure).

The first step in designing Kaleidoscope was formally defining the security guarantees that a poker protocol should achieve. Since such formal definitions are missing from current literature, we provide the first security definitions for poker in the so-called simulation paradigm, which is the gold standard for cryptographic protocol security. Our security definitions take into consideration all phases of a poker game, modeling the security guarantees obtained for each of them and the conditions under which they hold. Namely, we model security against very powerful adversaries who can attack all but one player. This worst case scenario also captures the case where many players in a game collude in order to cheat against one single player.

With a proper formal model in place, we developed Kaleidoscope, a highly efficient protocol that can be proven to realize our security definitions. Our protocol builds on cutting-edge zero knowledge proofs of shuffle correctness and is carefully crafted to achieve the best possible efficiency in terms of computation and communication. In fact, as shown in an upcoming work, Kaleidoscope achieves high security guarantees while requiring three times less computation and eight times less communication than the best previous protocols (without formal security guarantees).

Another important feature of Kaleidoscope is that it ensures that winners will receive their rewards, and that cheaters will be financially penalized as well as kicked out of the game. The basic idea is that, before a game starts all players send to a smart contract the funds they will be using for betting and an amount of "collateral" funds. At the end of the game, the smart contract ensures that the betting funds are distributed to the players according to the outcome of the game and that the collateral funds are returned. In case a player is caught cheating (which is ensured by our protocol), the smart contract confiscates the cheater's collateral funds and distributes those among the honest players as compensation. Moreover, we show that the communication with the smart contract and the on-chain storage requirements are minimal.

Although Kaleidoscope successfully addresses the three issues described above in the context of poker protocols, it can only be used to play poker games. There is a false common sense notion that poker protocols can be used for playing any other card games, which would actually lead to serious security issues. However, in the case of Kaleidoscope we were able to extend our formal security model, protocol and proofs to general card games. In doing so, we have obtained Royale, a protocol that can be securely used to play any card game with the same efficiency as Kaleidoscope. We will be describing Royale's features and techniques in an upcoming series of videos and blog posts.

creative commons