CERIAS

The Center for Education and Research in Information Assurance and Security

Public-Key Authentication Using Dessins d'Enfants

Jacob Bond

Dessins d'Enfants

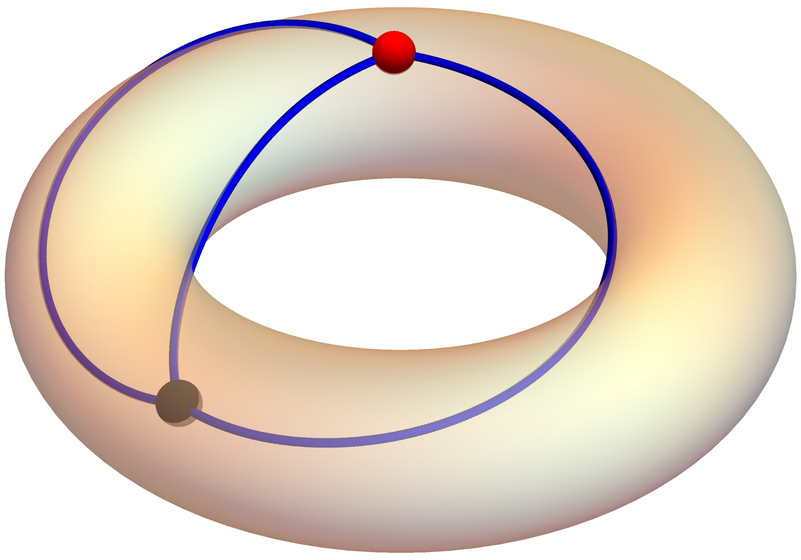
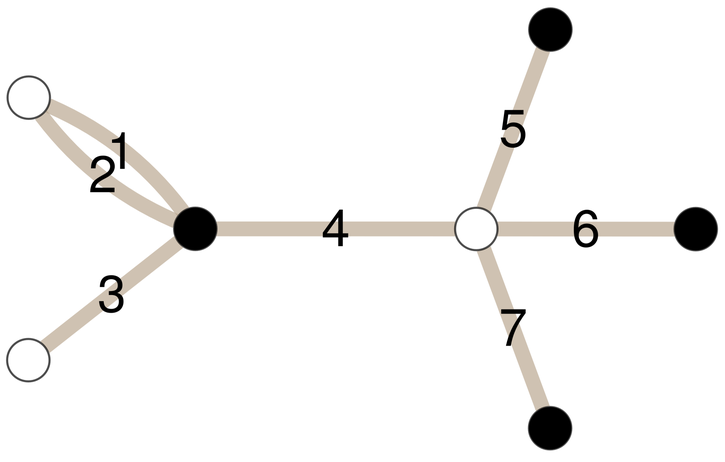


Figure 1: A dessin d'enfant drawn on a torus

A dessin d'enfant, French for "child's drawing", is a bipartite graph drawn without edge-crossings on a surface, such as a sphere or torus. Labeling the edges results in a cyclic ordering of the edges around each vertex, which can then be viewed as a pair of permutations $\sigma_0, \sigma_1 \in S_n$.



$$\sigma_0 = (1\ 2\ 3\ 4)\,(5)\,(6)\,(7)$$
$$\sigma_1 = (1\ 2)\,(3)\,(4\ 7\ 6\ 5)$$

Figure 2: A bipartite graph with edges labeled

Associated to each dessin d'enfant is a (class of) Belyĭ map(s), a function from the surface on which the dessin is drawn to the sphere, such as

$$\beta(x) = \frac{64x^3(x+1)}{(8x-1)}$$

or

$$\beta(x,y) = \frac{16 + y(x-5)}{32} \text{ on } E\colon y^2 = x^3 + 5x + 10.$$

By a result of Wood [1], it is possible to determine the dessin $\Delta_{\beta\circ\gamma}$ of a composition $\beta \circ \gamma$ from the dessins Δ_β of β and Δ_γ of γ.

Using Dessins for Cryptography

Given the Belyĭ map β, it is easy to compute the dessin Δ_β, but given the dessin Δ_β, it is difficult to compute the Belyĭ map β. It is this "one-wayness" that is exploited in this cryptographic protocol.

Suppose Alice knows β, Δ_β, while Bob knows γ, Δ_γ. Then Alice can give Bob Δ_β and Bob can give Alice Δ_γ, and they will both be able to compute $\Delta_{\beta\circ\gamma}$. However, neither will know both β and γ, because they cannot compute the Belyĭ map from the dessin.

$$\gamma, \Delta_\gamma : A \underset{\Delta_\beta}{\overset{\Delta_\gamma}{\rightleftarrows}} B : \Delta_\beta, \beta$$

The Protocol

Alice:
- private key: Belyĭ map γ on an elliptic curve E
- public key: dessin Δ_γ, elliptic curve E
- has a table $\{\gamma_i\}_i$ of Belyĭ maps on the sphere

Bob:
- chooses a challenge β, Δ_β on the sphere

$$A \xleftarrow{\ \beta\ } B$$

Alice randomly chooses $\gamma_1, \cdots, \gamma_n$ from her table and computes $\gamma_0 := \gamma_1 \circ \cdots \circ \gamma_n$, Δ_{γ_0}, and $\gamma_0 \circ \beta \circ \gamma$.

$$A \xrightarrow{\ \gamma_0 \circ \beta \circ \gamma,\ \Delta_{\gamma_0}\ } B$$

Bob computes $\Delta_{\gamma_0\circ\beta\circ\gamma}$ both from $\Delta_{\gamma_0}, \Delta_\beta, \Delta_\gamma$ and numerically from $\gamma_0 \circ \beta \circ \gamma$ and checks for agreement. He also performs a symbolic check to ensure Alice's response is consistent.

[1] Wood, M. Belyi-extending maps and the Galois action on dessins d'enfants. *Publ. Res. Inst. Math. Sci.* 42(3):721-737, 2006.

CERIAS

PURDUE UNIVERSITY