Elliptic Curve Verifiable Oblivious Pseudo-Random Function (EC-VOPRF) + CAPTCHA

Prof Bill Buchanan, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY

CAPTCHA

CAPTCHA

Network Working Group A. Davidson
Internet-Draft ISG, Royal Holloway, University of London
Intended status: Informational N. Sullivan
Expires: April 25, 2019 Cloudflare
C. Wood
Apple Inc.
October 22, 2018

Verifiable Oblivious Pseudorandom Functions (VOPRFs) in Prime-Order Groups
draft-sullivan-cfrg-voprf-02

Abstract

A Verifiable Oblivious Pseudorandom Function (VOPRF) is a two-party protocol for computing the output of a PRF that is symmetrically verifiable. In summary, the PRF key holder learns nothing of the input while simultaneously providing proof that its private key was used during execution. VOPRFs are useful for computing one-time unlinkable tokens that are verifiable by secret key holders. This document specifies a VOPRF construction instantiated within prime-order subgroups, including elliptic curves.

Status of This Memo

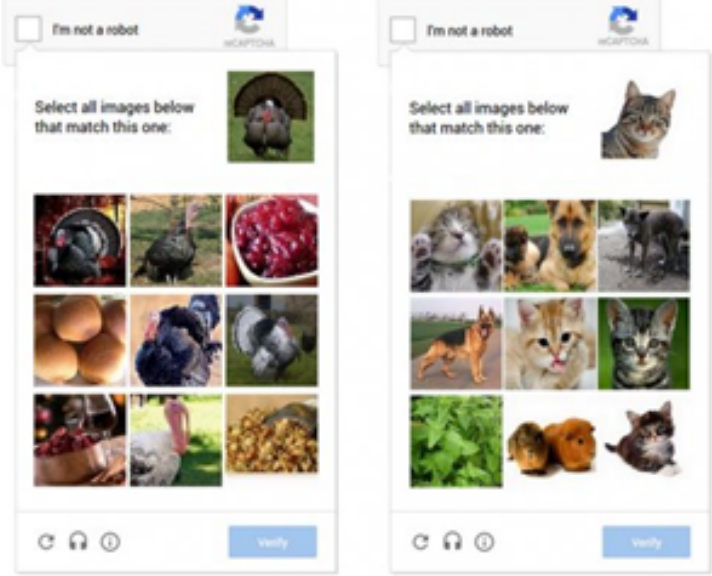
This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 25, 2019.

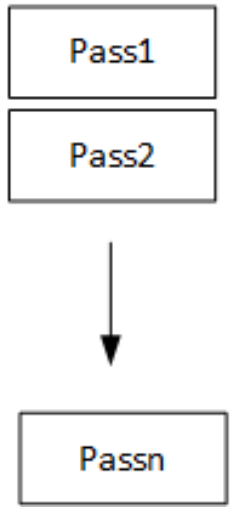
CAPTCHA


I'm not a robot
Select all images below that match this one:
Verify
I'm not a robot
Select all images below that match this one:
Verify

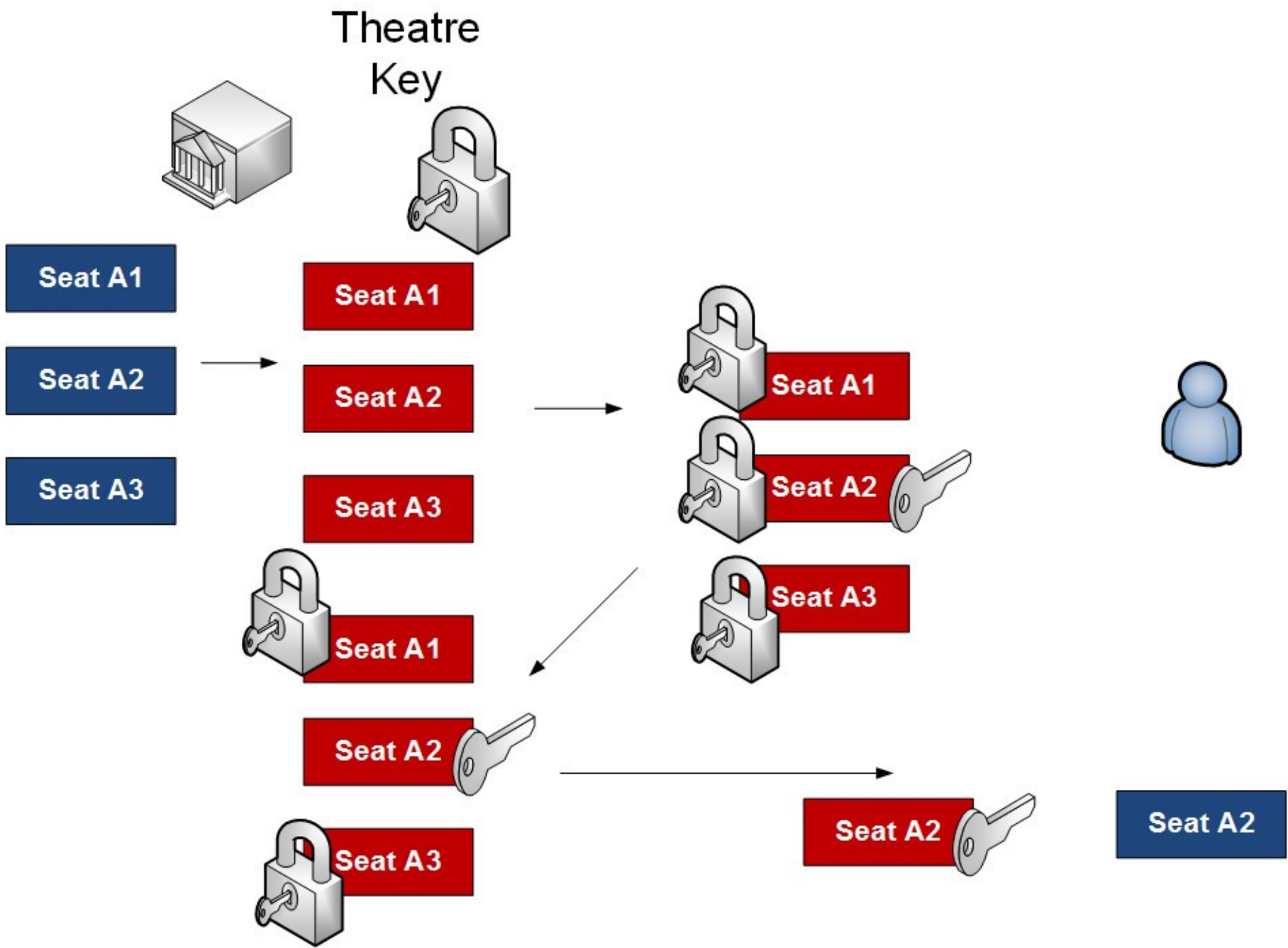

Bob


Tor
Network

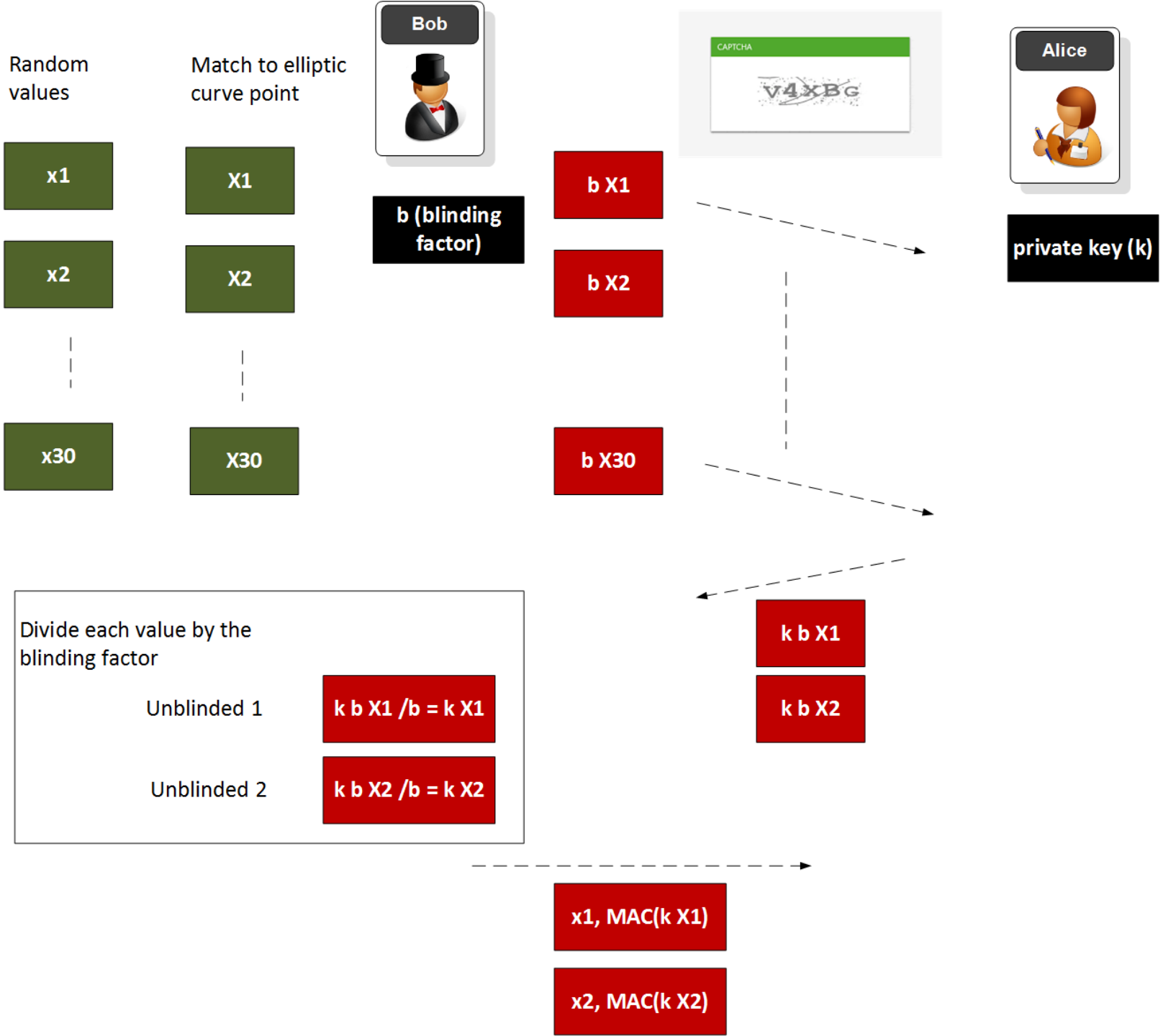

Alice


Pass1
Pass2
Passn

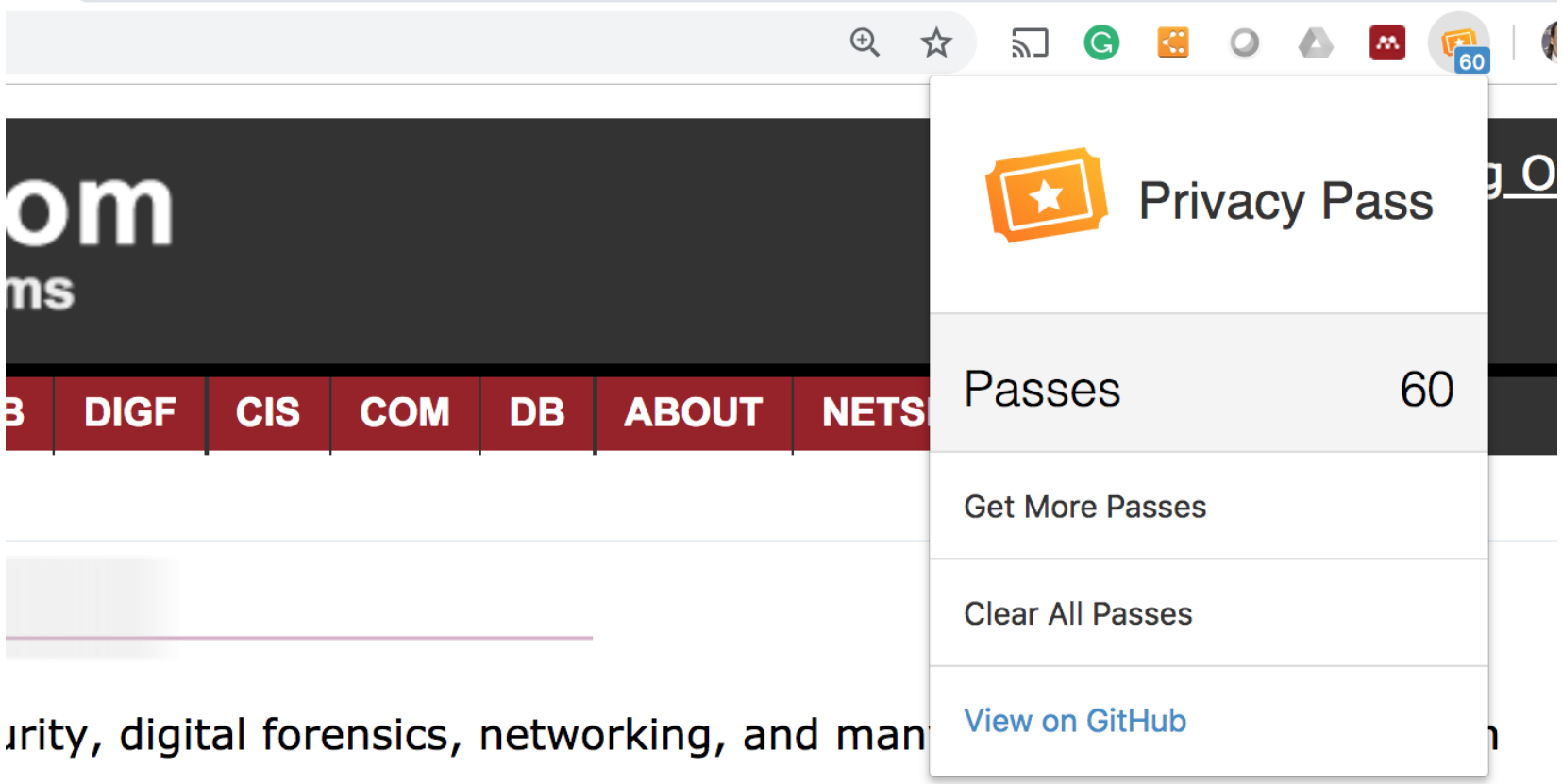
Oblivious Transfer



EC-VOPRF


Random values
Match to elliptic curve point
Bob
Alice
x1
x2
x30
X1
X2
X30
b (blinding factor)
b X1
b X2
b X30
CAPTCHA
V4XBG
private key (k)
k b X1
k b X2
Divide each value by the blinding factor
Unblinded 1
k b X1 /b = k X1
Unblinded 2
k b X2 /b = k X2
x1, MAC(k X1)
x2, MAC(k X2)

EC-VOPRF



Coding

This page contains a range of ciphers and codes, including Pigpen, Hashing (MD5, SHA-1) and Caeser Coding. Along with this it contains a calculator for the frequency analysis of ciphers.

Coding

Elliptic Curve Verifiable Oblivious Pseudo-Random Function (EC-VOPRF) + CAPTCHA

Prof Bill Buchanan, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY