



A Protocol for Privacy on the Internet

Alice and Bob had a chance meeting, was it in a chatroom, or perhaps through eBay. Their conversation is satisfactory, and they now wish some privacy. They want to retreat to a quiet virtual corner, and do some business, or talk candidly. But they know virtually nothing about each other, they have never met before, and all those “private chatrooms” offered to them, they know, are not really private.

That’s where PINprivate™ comes in: Alice prepares 1000 arithmetic exercises that each takes, say, 5 seconds to compute. She presents these exercises to Bob. Bob picks at random one exercise, say, exercise #371, and computes the result, say it is 7891. Bob sends the result of his exercise back to Alice. Alice who computed these tasks earlier knows from the result that Bob picked exercise #371. Both Alice and Bob compute exercise #371 to the next stage. When they have both done so they share the result of their computation, say, it is 57122. This number, 57122, is a shared secret between Alice and Bob. Harry, the hacker, has no clue that Bob picked exercise #371. He has to compute on average 500 tasks to realize that the number Bob sent to Alice (7891) indicates exercise #371. But that would be on average $500 \times 5 = 2500$ seconds later (some 40 minutes delay). Alice could in the meanwhile send Bob the password, or PIN, to an account she owns. Let’s say the PIN is: 24751. Alice will send Bob the number 81873 ($57122 + 24751$), from which Bob (but not Harry) will realize the password ($24751 = 81873 - 57122$), and access Alice’s account, then immediately change the password to it. When Harry, some 40 minutes later, comes along, it’s too late. Alice’s account may contain money she wishes to pay Bob, or perhaps a cryptographic key they would share from that moment on, securing their true privacy. This exchange between Alice and Bob is carried out through software. Alice and Bob only click their intent to establish bilateral privacy.

The chosen computational tasks are ‘one-way functions’. Their selection as well as the number of tasks, are cryptographically established. This protocol also offers a robust protection against abuse. Details are discussed in our white paper, available upon request.

PINprivate™ is part of PINSuite™ which also features: PINpay™: anonymity controlled OnLine Payment protocol; PINpen™: quick and secure log-on via a graphic interface; PINplan™: scaleable log-on security adjustable to ultra sensitive network circumstances; PINplay™: insuring honesty in on-line gaming, non repudiation, fairplay, and PINproof™: authenticating checks, hand-written, and hand-signed documents and drawings. Patents granted and pending.

Innovation by AGS Encryptions Ltd. (www.AGSgo.com)