Algebraic techniques for low communication secure protocols

Haan, R. de

Stellingen

behorende bij het proefschrift
"Algebraic Techniques for Low Communication Secure Protocols"
van Robbert de Haan

1. Multi-party computations for a large number of players become much more efficient when one uses a small number of dedicated servers to handle shares in the inputs of players and perform the necessary computations. Naturally, the correctness of the execution in this case relies on the capabilities of the adversary on these servers.

2. It is possible for 47 players to securely perform computations over $\mathbb{F}_2$ in the presence of a passive adversary corrupting up to 10 players, while only communicating $47 * 46 = 2162$ bits in total for every multiplication.
(*Consequence of Chapter 7*)

3. Assume a passive adversary and that players in an accepted set hold shares in some ramp scheme. Then it only takes a single round of communication for the players to convert their respective shares to shares for the same secret vector in any other ramp scheme with the same secret space. Furthermore, this communication can keep the secret private for any set of players that is rejected by both ramp schemes.

4. Fix a constant $n \in \mathbb{Z}_{>0}$ and take a two-phase perfectly secure message transmission protocol for $n = 2t + 1$ from this thesis. When one now slightly relaxes the value of t, i.e., assumes that $n = 2t + 1 + c$ for some $c \in \mathbb{Z}_{>0}$, one can achieve a linear factor $c + 1$ improvement on the overhead of the selected protocol.

5. The regulator of a real quadratic field $\mathbb{Q}(\sqrt{D})$ can be computed unconditionally in expected time $O(D^{1/6+\epsilon})$ under the Generalized Riemann Hypothesis.
(*de Haan, Jacobson, Jr. and Williams. Math. Comp, vol. 76, pp. 2139–2160*)

6. Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field, $I = (Q, P)$ with $Q, P \in \mathbb{Z}$ be a reduced primitive ideal in the ring $\mathcal{O}_K$ of integers in K.[1] For $i \in \mathbb{Z}_{>0}$, let the reduced primitive ideal $I_i = (Q_i, P_i) = (\Psi_i)I$ correspond with the value $\psi_i = (P_i + \sqrt{D})/Q_i$ resulting from i applications of the continued fraction algorithm to the value $\psi = (P+\sqrt{D})/Q$. Then $\Psi_{i+m} > F_{m+1}\Psi_i$, where $m \geq 1$, $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.
(*de Haan, Jacobson, Jr. and Williams. Math. Comp, vol. 76, pp. 2139–2160*)

7. Accepting a hash made using MD5 is no longer just a bad idea, but now also often provably harmful.

8. As $q \to \infty$, the function $f(x) = 1 - H_q(x)$ approaches the line $g(x) = 1 - x$ for $0 < x < 1 - 1/q$.

9. One cannot fully know how well one controls a foreign language until one has spent some time in a country where this language is native.

10. In many restaurants it is not unusual for dessert to be the first dish to arrive at the table.

11. When a Canadian inquires how you are doing, this does not indicate that he or she necessarily expects (or wants) a response.

[1] We use the notation (Q, P) with $Q|(D - P^2)$ here as shorthand for the ideal $[Q/\sigma, (P + \sqrt{D})/\sigma]$ where $\sigma = 2$ if $D \equiv 1 \pmod 4$ and $\sigma = 1$ otherwise.