Privatsphäre-bewahrende Smart Grids via Secure Multi-Party Computation

BERGISCHE UNIVERSITÄT WUPPERTAL

Smart Grids

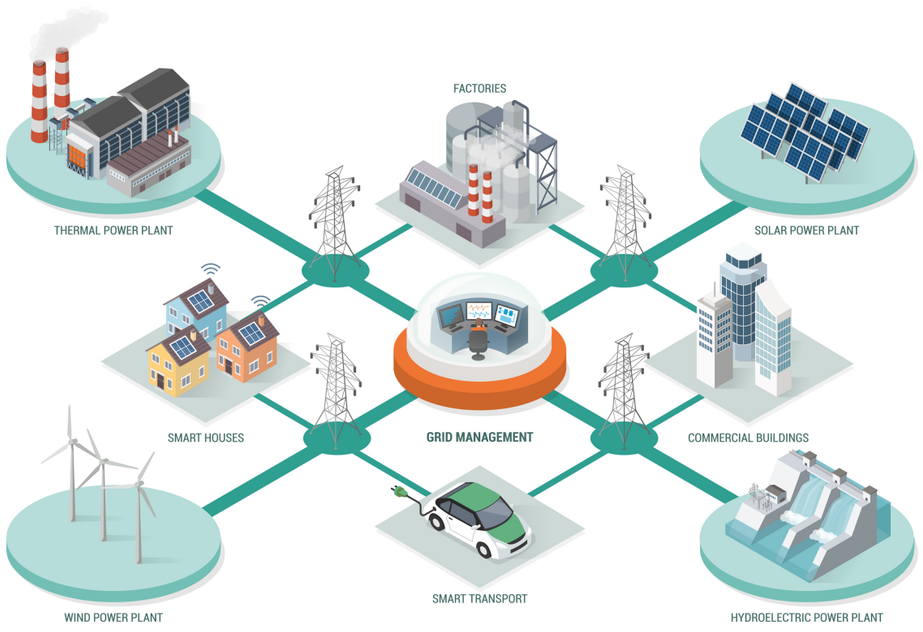

Abbildung 1. Illustration eines Smart Grids.

Die Energiewende stellt die öffentliche Energieversorgung vor neue Herausforderungen: Zukünftig wird der Großteil unserer Energie aus Quellen kommen, die nicht zuverlässig und konstant Strom erzeugen, sondern fluktuierend, wie z.B. Solarenergie oder Windkraft. Um dennoch eine sichere, zuverlässige und günstige Versorgung mit Energie zu ermöglichen, ist es sinnvoll, auf intelligente Energienetze umzustellen, sogenannte "Smart Grids". In Smart Grids wird die Stromverteilung durch multilateralen Austausch von Strom (z.B. von Solaranlagen, Batterien und Elektroautos) und Daten (z.B. Verbrauchsprognosen, Nutzungsdaten, etc.) zwischen Betreiber und Abnehmern optimiert. Dies ermöglicht es dem Energienetzbetreiber vorausschauend zu planen und Effizienzrenditen zu erzielen. Außerdem ermöglichen es Smart Grids, die Energienetze nicht wie bisher üblich ausschließlich durch Steuerung des Angebots zu regeln, sondern auch durch Steuerung der Nachfrage, z.B. durch dynamische Preisgebung. Somit stellen Smart Grids eine effizientere und robustere Alternative zu herkömmlichen Energienetzen dar.

Datenschutz in Smart Grids

Leider stehen der flächendeckenden Einführung von Smart Grids Datenschutzbedenken entgegen. Durch die eng getatktete Stromverbrauchsabfrage sowie das Senden von Verbrauchsprognosen erhält der Netzbetreiber detaillierte Einsicht in die Aktivitäten der Nutzer. Während herkömmliche Stromnetze lediglich den monatlichen Gesamtverbrauch eines Haushalts erfassen, nutzen intelligente Stromnetze in der Regel sogenannte *Smart Meter*, welche detaillierte Verbrauchsdaten liefern. Untersuchungen haben gezeigt, dass selbst ohne *a priori*-Kenntnis von Haushaltsgeräten komplexe Nutzungsmuster identifiziert werden können, darunter Anwesenheit, Anzahl der Bewohner und Tagesablauf. Die Daten der Smart Meter erlauben aufgrund der Schwankungen im Stromverbrauch beim Anzeigen heller und dunkler Szenen audiovisueller Inhalte sogar Rückschlüsse darüber, welche Filme geguckt werden.

Zur Lösung dieser Probleme können kryptographische Techniken wie **Secure Multi-Party Computation (MPC)** eingesetzt werden.

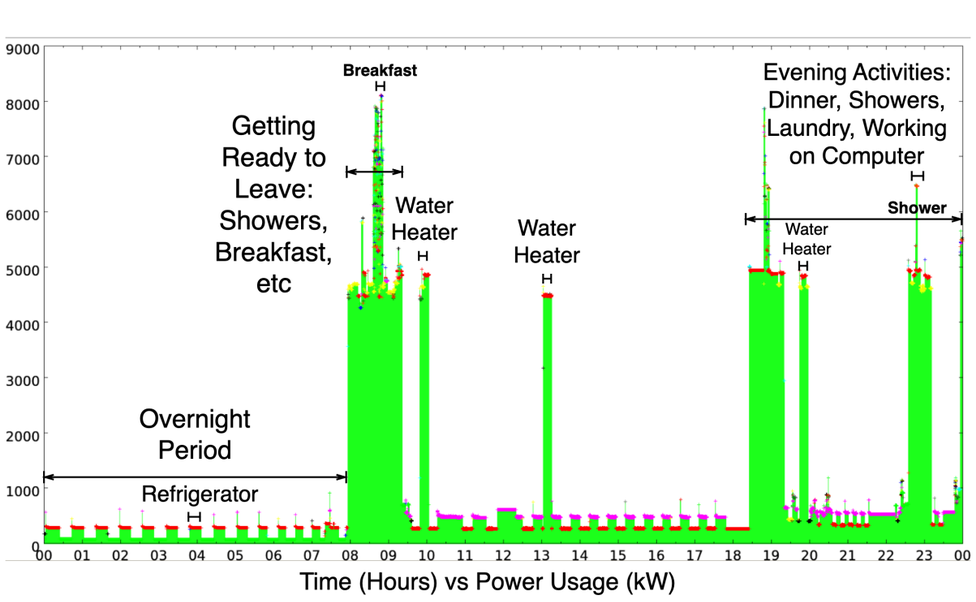

Abbildung 2. Nutzung von Stromverbrauchsdaten zur Rekonstruktion des Tagesablaufs eines Privathaushalts (von Molina-Markham et al., *Private Memoirs of a Smart Meter*, BuildSys 2010).

Secure Multi-Party Computation

Multi-Party Computation (MPC) ermöglicht es einer Gruppe von n Teilnehmern verteilte Berechnungen durchzuführen, zu der jeder Teilnehmer eine Eingabe beisteuert ohne diese offenbaren zu müssen (siehe Abbildung 3).

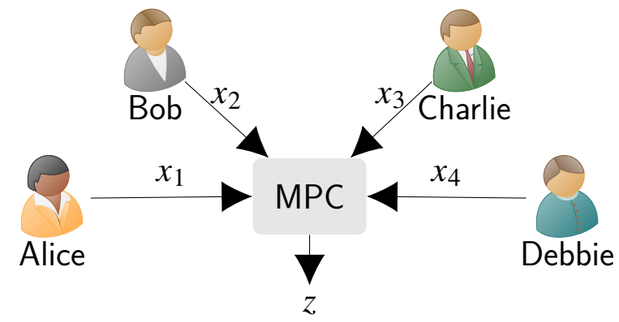

Abbildung 3. Sichere verteilte Berechnung einer Funktion $f(x_1, \ldots, x_4) = z$ zwischen $n = 4$ Parteien.

Teilnehmer, die sich zusammenschließen, um Informationen über die geheimen Eingaben anderer zu erfahren, heißen *dishonest*. Je nach verwendeten MPC-Protokoll ist die Berechnung sicher, so lange höchstens $\lfloor n/2 \rfloor$ bzw. $n - 1$ Teilnehmer dishonest sind; man spricht dann von Sicherheit ggü. einer *honest* bzw. einer *dishonest majority*. Teilnehmer, die *dishonest* sind, werden entweder als *semi-honest*- (auch *honest-but-curious*) oder *malicious* klassifiziert. Wenn sie semi-honest sind, befolgen sie das Protokoll exakt, tauschen aber untereinander Informationen aus, um geheime Eingaben anderer Teilnehmer zu rekonstruieren. Wenn sie malicious sind, können sie zusätzlich beliebig vom Protokoll abweichen. Ein MPC-Protokoll ist *korrekt*, wenn $z = f(x_1, \ldots, x_n)$ gilt, und *sicher*, wenn keine Partei mehr erfährt als z.

Privatsphäre-bewahrende Lastflussanalyse

In Smart Grids liefert die **Lastflussanalyse** (LFA) entscheidende Informationen über die Netzperformance und trägt dazu bei, Probleme wie Spannungsinstabilität und Überlastungen zu vermeiden. Zugleich stützt sich die LFA auf Leistungsprognosen, die aus Verbrauchsdaten gewonnen werden und potenziell sensible Rückschlüsse auf das Nutzerverhalten erlauben. Um dieses Dilemma zu lösen, haben wir eine **privatsphäre-bewahrende Lastflussanalyse** auf Basis von MPC implementiert und evaluiert. Dabei werden die nichtlinearen Gleichungssysteme zunächst mittels dem Newton-Verfahren linearisiert und anschließend entweder per LU-Zerlegung oder mit der *Generalized Minimal Residual*-Methode (GMRES) gelöst. Wie Tabelle 1 zeigt, liegen die Laufzeiten unserer Benchmarks – abhängig von Netzlatenz, Sicherheitsmodell und Netzgröße – zwischen 30 s und 30 min. Damit ist unsere Implementierung beispielsweise in Flexibilitätsmärkten praktikabel, in denen LFA genutzt wird, um Spannungsbandverletzungen innerhalb eines 24-Stunden-Intervalls vorherzusagen.

Tabelle 1. Laufzeit in Sekunden (* schnellste and † langsamste)

Round-trip Latenz (in Milisekunden)	Semi-honest, honest majority LU	Semi-honest, honest majority GMRES	Semi-honest, dishonest majority LU	Semi-honest, dishonest majority GMRES	Malicious, dishonest majority LU	Malicious, dishonest majority GMRES
städtisches Netz mit $n = 39$						
1	72	111	62*	114	450	199
5	2,227	3,549	280	535	2,701	1,073
10	2,227	3,624	566	1,075	3,993†	1,672
Ländliches Netz mit $n = 13$						
1	27*	41	56	92	52	85
5	102	163	300	498	218	364
10	197	316	566	935†	420	700

Ausblick

Der Flaschenhals vieler MPC-Verfahren ist die hohe Zahl von Kommunikationsrunden, welche insbesondere in Smart Grids mit hoher Netzlatenz den effizienten Einsatz von MPC erschweren. Um den Einsatz privatsphäre-bewahrender Verfahren in solchen Netzen zu ermöglichen, arbeiten wir derzeit an *rerandomizable garbling schemes*, die MPC mit konstanter Anzahl von Kommunikationsrunden erlauben.

Veröffentlichtes Paper

von der Heyden et al., *Privacy-Preserving Power Flow Analysis via Secure Multi-Party Computation*, IEEE Transactions on Smart Grid, 2025.

Unser Paper zeigt, wie der Einsatz von MPC es ermöglicht, Lastflussanalyse privatsphäre-bewahrend durchzuführen.

Chair for IT-Security and Cryptography
Bergische Universität Wuppertal
Germany
itsc.uni-wuppertal.de

Read our paper:
arxiv.org/abs/2411.14557