FORSCHUNG KOMPAKT

Neuartige Bauelemente

Hardware-Sicherheit: Mehrdimensional geschützt

Ob digitale Stromzähler oder Tachometer: Werden Verbrauch oder Laufleistung elektronisch ausgelesen, sollten die übermittelten Daten nicht manipulierbar sein. Das gilt in besonderem Maße für die Verifizierung von Zahlungstransfers mittels Kreditkarte. Am Fraunhofer-Institut für Photonische Mikrosysteme IPMS haben Forschende eine Lösung entwickelt, die es ermöglicht, die Funktion entsprechender Sicherheitselemente nach der Herstellung zu konfigurieren und diese so zuverlässig und kostengünstig mehrdimensional zu schützen.

Über Von Zahlungstransfers bis zu digitalen Stromzählern – für diese komfortablen, elektronisch auslesbaren Vorgänge ist entscheidend, dass die dahinterstehenden Produkte nicht manipuliert werden können. Hierfür sorgen verschlüsselte Identifikationen oder Betriebsprotokolle in den elektronischen Schaltkreisen. Zunehmend stellt sich jedoch die Herausforderung, dass diese Sicherheitselemente umgangen werden können. Konventionelle Lösungen wie Hardware-Security-Module (HSM) oder Datenbanken gewährleisten nur eine relative Sicherheit – und sind zudem kostenintensiv. Dr. Maximilian Lederer vom Fraunhofer IPMS und seinem Team ist es gelungen, einen in mehrerlei Hinsicht vielversprechenden Lösungsweg aufzuzeigen.

Mit Kristallisation mehrdimensional verschleiern

Das Projekt der Fraunhofer IPMS-Fachleute basiert auf einem Effekt, den die Expertinnen und Experten erstmals 2020 beobachteten: Sie entdeckten, dass Hafniumoxid unter Anlegung eines elektrischen Wechselfeldes kristallisieren kann. Der Stoff wird dadurch ferroelektrisch, das heißt, er kann eine spontane elektrische Polarisation erzeugen und wie ein Lichtschalter zwischen Speicherzuständen hin- und herschalten.

Auf Basis dieser Entdeckung gestalten die Fraunhofer-Fachleute Bauelemente, die über diese durch ein elektrisches Feld induzierte Kristallisation (FINK) ihr ferroelektrisches Verhalten gezielt ändern können. Da die ferroelektrische Polarisation nicht extern auszulesen ist, ermöglicht das Verfahren eine besondere Sicherung: »Wir schaffen ein System zur mehrdimensionalen Verschlüsselung von Hardware, indem wir in unsere FINK-Bauelemente drei Eigenschaften einspeichern: den Grad der Kristallisation, die Höhe der Polarisation, das heißt, die vorliegende ferroelektrische Phase und zu welchem Anteil man sie einprogrammiert, und in dritter Instanz das Vorzeichen dieser Phase. Das lässt sich auch in verschiedenen Größen abbilden, der Permittivität und der Ladung«, erläutert Projektleiter Lederer.

Kontakt
Monika Landgraf | Fraunhofer-Gesellschaft, München | Kommunikation | Telefon +49 89 1205-1333 | presse@zv.fraunhofer.de
Franka Balvin | Fraunhofer-Institut für Photonische Mikrosysteme IPMS | Telefon +49 351 8823-1144 | Maria-Reiche-Straße 2 | 01109 Dresden | www.ipms.fraunhofer.de | franka.balvin@ipms.fraunhofer.de

Sicher in der Hand der Hersteller

Üblicherweise senden Hersteller von Halbleitern, die über keine eigene Fertigung verfügen, ihr System-Schaltkreisdesign an externe Auftragsfertiger, teilen entsprechend mit diesen auch die IP und bekommen das fertige Bauelement zurück. Nachteile dieser Vorgehensweise: Die Funktion einer Schaltung ist nicht mehr zu ändern, Sicherheitsmerkmale sind entweder festverdrahtet oder Software-basiert, weshalb Manipulationen oder Fälschungen schwer erkannt werden können. Zudem sind diese Lösungen sehr teuer und nur in Kleinserien einsetzbar. Nicht so beim FINK-Verfahren: »Mit unserer Lösung werden Funktion und Eigenschaften der integrierten Schaltung beim ideengebenden Unternehmen definiert, an die Fabrikation transferiert und dort mit dem FINK-Bauelement gefertigt, ohne dass die dahinterstehende IP geteilt werden muss. Halbleiterhersteller können die Funktion einer Schaltung durch die elektrischen Signale, die sie anlegen, nach der Herstellung selbst konfigurieren«, unterstreicht Lederer. Die Forschenden wollen ihre Bauelemente in moderne Mikroelektronik-Prozessflüsse integrieren, damit ideengebende Kunden am Ende immer selbst entscheiden können, wie ihre Verschlüsselung aussieht. Das ist vor allem interessant für Anwendungen im Bereich von Automotive und HSM-Chips, welche zum Beispiel bei Banktransfers angesetzt werden.

Die Fraunhofer-IPMS-Fachleute sind überzeugt: Der FINK-Ansatz ebnet den Weg für die massentaugliche Fertigung integrierter Sicherheitsmerkmale. Hinzu kommt, dass FINK-Schaltkreise im Gegensatz zu gängigen programmierbaren integrierten Pendants kostengünstiger und leistungsfähiger bei niedrigem Stromverbrauch sind, da geringe Spannungen ausreichen, um die dreidimensionalen Zustände von FINK-Elementen zu schreiben.

Zuverlässig und mit besten Aussichten

Aktuell erbringen die Forschenden den Nachweis, dass ihre Lösung nicht nur im Labormaßstab, sondern auch im integrierten System funktioniert. Die bisherigen Ergebnisse können sich sehen lassen, potenzielle Hürden wurden mit Bravour genommen. So hatten Lederer und sein Team zunächst Sorge, dass die Temperaturstabilität eine größere Herausforderung darstellen könnte, da der FINK-Prozess thermisch abhängig ist. »Wir konnten nachweisen, dass der Effekt zwar temperaturabhängig ist, die Zuverlässigkeit der danach erstellten Schicht, beziehungsweise des Bauelements jedoch auch bei verschiedenen Temperaturen konstant bleibt. Das heißt, wir sehen keine temperaturabhängigen Verluste«, freut sich der Projektleiter.

Die FINK-Technologie bietet nicht nur überzeugende Entwicklungsmöglichkeiten für hochsichere und zugleich kostengünstige Halbleiterlösungen. Durch die Kompatibilität des eingesetzten Hafniumoxids mit bestehenden Halbleiterfertigungstechnologien sehen die Fachleute zudem großes Potenzial hinsichtlich einer schnellen Überführung in die industrielle Anwendung.

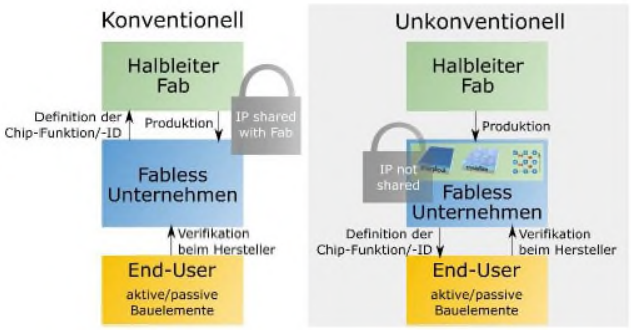

Abb. 1 Schematische Darstellung des bisherigen Verfahrens und des neuen im FINK-Projekt vorgeschlagenen Verfahrens für die Verschlüsselung bzw. Funktionsdefinition von integrierten Schaltungen.

© Maximilian Lederer, Fraunhofer IPMS