RKD

Lösung für die Erzeugung und Verteilung von kryptografischen Schlüsseln auf Basis von Funkkanaleigenschaften

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS-K-Pass-KMU Innovation AKUT KIA F&E Dienstleistungen (FED KIA_2023)	**Status**	abgeschlossen
Projektstart	01.07.2024	**Projektende**	31.08.2025
Zeitraum	2024 - 2025	**Projektlaufzeit**	14 Monate
Keywords	IT-Sicherheit, Kryptografie, Schlüsselverteilung		

Projektbeschreibung

Digitalisierung, Globalisierung und Vernetzung benötigen eine sichere Telekommunikation und diese wiederum erfordert eine sichere Kryptografie. Durch die zukünftigen Quantencomputer sind neue Verfahren der Kryptografie erforderlich, wie Post-Quanten-Kryptografie, QKD (Quantum Key Distribution) und RKD (Radio-signal Key Distribution). Im vorliegenden Projekt wird die weltweit erste Lösung für RKD auf Ebene TRL 7 für kleine Entfernungen (mit Direktfunk) und große Entfernungen (via Satelliten) entwickelt und demonstriert. Die dahinterliegende Technologie entstand in den Forschungsprojekten KIF (KIRAS) und LoRaKey (Bridge) und auf Basis des Standes der Technik.

Abstract

Digitalization, globalization and networking require secure telecommunications, which in turn require secure cryptography. Future quantum computers will require new cryptography methods, such as post-quantum cryptography, QKD (quantum key distribution) and RKD (radio-signal key distribution). This project is developing and demonstrating the world's first solution for RKD at TRL 7 level for short distances (with direct radio) and long distances (via satellite). The underlying technology was developed in the KIF (KIRAS) and LoRaKey (Bridge) research projects and is based on the state of the art.

Endberichtkurzfassung

RKD - Lösung für die Erzeugung und Verteilung von kryptografischen Schlüsseln auf Basis von Funkkanaleigenschaften

Es wurde im Projekt RKD die weltweit erste Lösung für RKD (Radio-signal Key Distribution) auf Ebene TRL 7 für kurze Entfernungen (mit Direktfunk) entwickelt und demonstriert.

Die Digitalisierung, Globalisierung und weltweite Vernetzung benötigen eine sichere Telekommunikation und Datenspeicherung und diese wiederum erfordern eine sichere Kryptographie. Mit dem Erscheinen von geeigneten Quantencomputern ist in Zukunft die heutige asymmetrische Kryptografie aus Sicherheitsgründen nicht mehr verwendbar. Diese Problematik ist heute schon relevant für langlebig ausgelegte Infrastrukturen (Verkehr, Industrie etc.), größere Softwaresysteme (sind im Kern meist langlebig ausgelegt) sowie für Daten, wo eine langzeitige Vertraulichkeit wichtig ist.

Wenn das Vertrauen in mathematische Verfahren, wie der Post Quanten Kryptografie, nicht ausreicht, müssen physikalische Verfahren eingesetzt werden, was für die Erzeugung und Verteilung kryptografischer Schlüssel möglich ist. Neben QKD (Quantum Key Distribution) bietet dafür RKD (Radio-signal Key Distribution) eine geeignete Lösung. QKD gilt zwar als eine hochsichere Lösung für die Erzeugung und Verteilung kryptografischer Schlüssel, jedoch stehen ihrer praktischen Implementierung erhebliche wirtschaftliche Hürden entgegen. Die benötigte hochspezialisierte Hardware macht QKD äußerst kostspielig. Demgegenüber ist RKD sehr kostengünstig und robust. Die erforderliche Hardware basiert auf kommerziell verfügbaren LoRa-Modulen oder Software Defined Radios (SDRs), die inklusive Energieversorgung, Gehäuse und Software bereits ab circa € 200 pro Gerät erhältlich sind. Diese kostengünstigen Komponenten ermöglichen sowohl die Funkübertragung als auch die präzise Erfassung der für die Schlüsselgenerierung erforderlichen Kanalmessungen bis hin zum endgültigen hochsicheren (nichtdeterministischen) kryptografischen Schlüssel.

Es ist mit RKD sehr kostengünstig und massentauglich die zufällige Erzeugung und hochsichere Verteilung von symmetrischen Schlüsseln möglich. Und das gilt vor allem für bewegliche Objekte, wie Geräte bei Verkehrsinfrastrukturen (Straße, Schiene, Wasser, Luft), beweglichen IoT-Geräten, Drohnen, militärische Einheiten etc., weil RKD für die Schlüsselerzeugung eine Dynamik des Umfeldes benötigt. Der Nachteil von RKD ist die langsame Schlüsselerzeugung, die sich aus den Dynamikanforderungen ergibt - maximal einige Bits pro Sekunde sind möglich.

Bei RKD (Radio-signal Key Distribution) senden zwei Kommunikationsgeräte (Alice und Bob) halbwegs gleichzeitig Funksignale mit Frequenzen über 30 MHz in beide Richtungen und messen dabei kontinuierlich die empfangenen Signaleigenschaften. Das zentrale Prinzip liegt in der Reziprozität des Funkkanals: Da beide Geräte denselben physikalischen Übertragungsweg nutzen, messen sie nahezu identische Kanaleigenschaften. Diese gemeinsamen Messwerte bilden die Grundlage für die Generierung identischer kryptographischer Schlüssel auf beiden Seiten, ohne dass diese Informationen über einen separaten Kanal ausgetauscht werden müssen. Mit RKD entstehen auf beiden Seiten (A und B) gleiche nichtdeterministische Zufallszahlen, die ihre Entropie direkt aus den physikalischen Eigenschaften der Funkübertragung beziehen. Die Zufälligkeit der Schlüssel ergibt sich aus dem Übertragungsweg der Funksignale (der inhärenten Unvorhersehbarkeit) und kann von einem Dritten (Angreifer) nicht gemessen werden. Änderungen der Messungen entstehen vor allem durch die Dynamik des Übertragungsweges (Reflexionen etc.) und der Bewegung auf zumindest einer Seite (Entfernungsänderungen). Es ist kein zusätzlicher nichtdeterministischer Zufallszahlengenerator erforderlich, weil sich die Zufälligkeit aus den Messwerten ergibt.

Praktische Tests im Projekt RKD haben gezeigt, dass koordinierte räumliche Angriffe in realen Umgebungen durch Dritte, die ebenfalls diese Messungen durchführen, zu keinem Erfolg führen, insbesondere bei den typischen Mobilitätsszenarien, für die RKD primär konzipiert ist. Experimentelle Validierungen unter kontrollierten Bedingungen haben im Projekt RKD gezeigt, dass bereits bei Abständen von 50 cm bis 1 m zwischen dem Angreifer und den legitimen Kommunikationspartnern eine signifikante räumliche Dekorrelation der Kanalmessungen auftritt. In diesen Worst-Case-Szenarien weist der Angreifer schon eine zwei- bis dreifach höhere Bitfehlerrate gegenüber den beiden legitimen Kommunikationspartnern auf, was die Lokalität der Kanalcharakteristik bestätigt.

Das Ergebnis des Projektes RKD ist eine vollständige Lösung auf Ebene TRL7 (TRL8 ohne Zertifizierung) für die kostengünstige und massentaugliche hochsichere physikalische Erzeugung und Verteilung kryptografischer Schlüssel für kurze Entfernungen, die nach den erforderlichen Zertifizierungen einem internationalen Marketing zugeführt wird. Die

wesentliche Limitation von RKD liegt in der geringen Schlüsselgenerierungsrate, die systembedingt auf maximal 2 bis 8 Bits pro Sekunde beschränkt ist. Diese Einschränkung resultiert aus den erforderlichen Dynamikanforderungen des Systems und der notwendigen Korrelationszeit zwischen den Kanalmessungen.

Projektleiterin: DI Eva Sophie Wiesmüller

Entwicklungsleiter: DI Dr. Ernst Piller

ProjektpartnerInnen (Bedarfsträger): Bundeskanzleramt, Bundesministerium für Landesverteidigung

Kontakt: insitu software gmbh, Heinrich Schneidmadl Strasse 15, 3100 St. Pölten
Tel.: 0676 433 7123
wiesmueller@insitu.software , piller@insitu.software , www.insitu.software

RKD – Solution for the generation and distribution of cryptographic keys based on radio channel properties

The RKD project developed and demonstrated the world's first solution for RKD (Radio Signal Key Distribution) at TRL 7 for short distances (with terrestrial connection).

Digitalisation, globalisation and global networking require secure telecommunications and data storage, which in turn require secure cryptography. With the advent of suitable quantum computers, today's asymmetric cryptography will no longer be usable in the future for security reasons. This problem is already relevant today for long-lasting infrastructures (transport, industry, etc.), larger software systems (which are usually designed to be long-lasting at their core) and for data where long-term confidentiality is important. If trust in mathematical methods such as post-quantum cryptography is insufficient, physical methods must be used, which is possible for the generation and distribution of cryptographic keys. In addition to QKD (quantum key distribution), RKD (radio signal key distribution) offers a suitable solution for this. Although QKD is considered a highly secure solution for the generation and distribution of cryptographic keys, there are considerable economic hurdles to its practical implementation. The highly specialised hardware required makes QKD extremely expensive. In contrast, RKD is very cost-effective and robust. The necessary hardware is based on commercially available LoRa modules or software-defined radios (SDRs), which are available from around € 200 per device, including power supply, housing and software. These low-cost components enable both radio transmission and precise recording of the channel measurements required for key generation, right through to the final highly secure (non-deterministic) cryptographic key.

RKD enables the random generation and highly secure distribution of symmetric keys in a very cost-effective and mass-marketable way. This is especially true for moving objects, such as devices in transport infrastructure (road, rail, water, air),

mobile IoT devices, drones, military units, etc., because RKD requires a dynamic environment for key generation. The disadvantage of RKD is the slow key generation resulting from the dynamic requirements – a maximum of a few bits per second are possible.

With RKD (Radio-signal Key Distribution), two communication devices (Alice and Bob) transmit radio signals with frequencies above 30 MHz in both directions at roughly the same time, continuously measuring the received signal properties. The central principle lies in the reciprocity of the radio channel: since both devices use the same physical transmission path, they measure almost identical channel properties. These shared measurements form the basis for generating identical cryptographic keys on both sides without having to exchange this information via a separate channel. With RKD, identical non-deterministic random numbers are generated on both sides (A and B), which derive their entropy directly from the physical properties of the radio transmission. The randomness of the keys results from the transmission path of the radio signals (the inherent unpredictability) and cannot be measured by a third party (attacker). Changes in the measurements are mainly caused by the dynamics of the transmission path (reflections, etc.) and movement on at least one side (changes in distance). No additional non-deterministic random number generator is required because the randomness results from the measured values.

Practical tests in the RKD project have shown that coordinated spatial attacks in real environments by third parties who also perform these measurements are unsuccessful, especially in the typical mobility scenarios for which RKD is primarily designed. Experimental validations under controlled conditions in the RKD project have shown that significant spatial decorrelation of the channel measurements already occurs at distances of 50 cm to 1 m between the attacker and the legitimate communication partners. In these worst-case scenarios, the attacker already has a two to three times higher bit error rate compared to the two legitimate communication partners, which confirms the locality of the channel characteristics.

The result of the RKD project is a complete solution at TRL7 (TRL8 without certification) for the cost-effective and mass-marketable, highly secure physical generation and distribution of cryptographic keys for short distances, which will be marketed internationally after the necessary certifications have been obtained. The main limitation of RKD is the low key generation rate, which is limited to a maximum of 2 to 8 bits per second due to the system. This limitation results from the necessary dynamic requirements of the system and the necessary correlation time between the channel measurements.

Project manager: DI Eva Sophie Wiesmüller

Head of development: DI Dr Ernst Piller

Project partners: Federal Chancellery, Federal Ministry of Defence

Contact: insitu software gmbh, Heinrich Schneidmadl Strasse 15, 3100 St. Pölten
Tel.: 0676 433 7123
wiesmueller@insitu.software , piller@insitu.software , www.insitu.software

Projektkoordinator

- insitu software gmbh

Projektpartner

- Bundesministerium für Landesverteidigung
- Bundeskanzleramt