



Post-Quantum Kryptographie für IPsec

Dipl.-Inf. Ephraim Zimmer

24. Februar 2015



Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG







Peter Shor - 1994

“Algorithms for Quantum Computation: Discrete Logarithms and Factoring”

© D-Wave Systems Inc.

Peter Shor - 1994

"Algorithms for Quantum Computation: Discrete Logarithms and Factoring"



Post-Quantum Kryptographie

© D-Wave Systems Inc.

Notwendige Schritte



IPsec Analyse



Geeignete Kryptosysteme für PQC



PQC-Implementierung



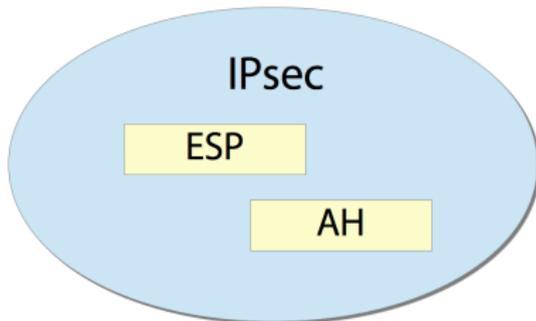
IPsec Erweiterung



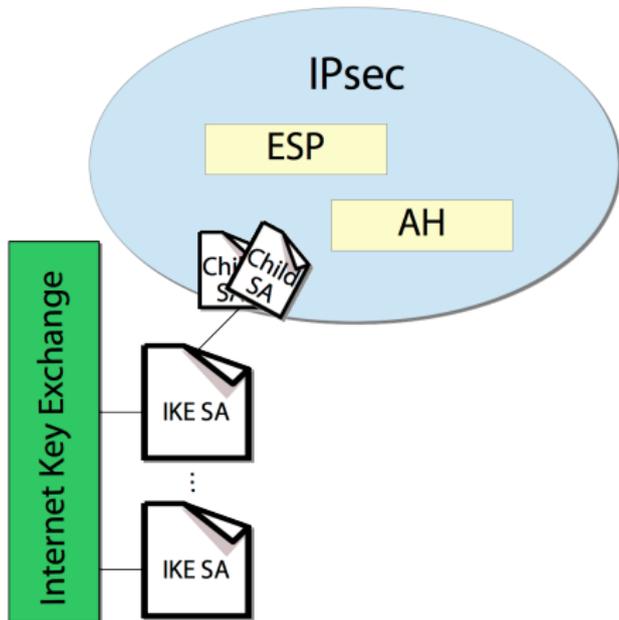
Evaluation und Vergleich



IPsec Analyse

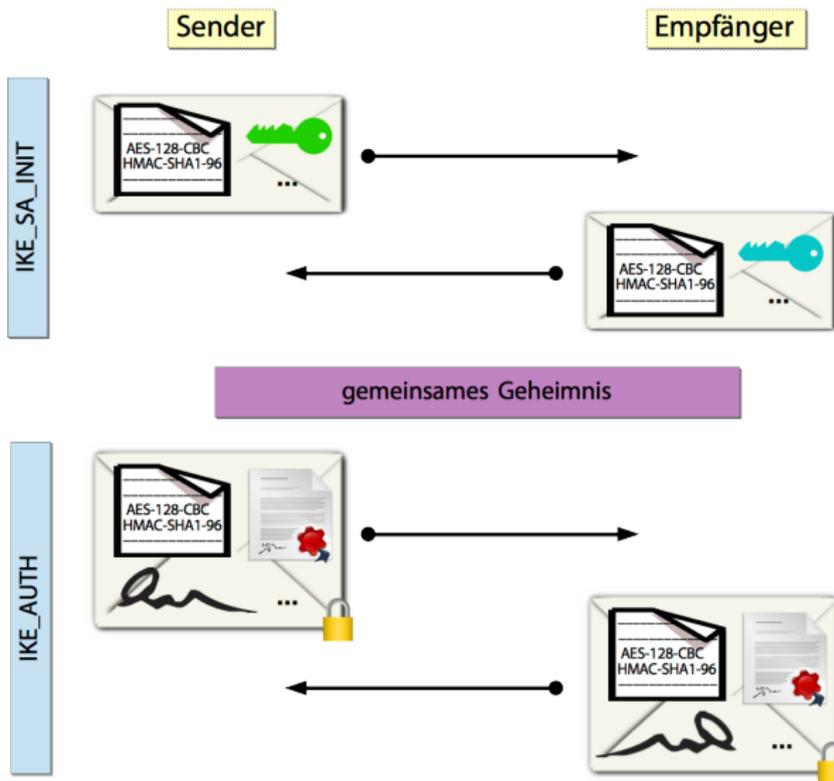


- Zugriffskontrolle
- Teilnehmerauthentifizierung
- verbindungslose Integrität
- Vertraulichkeit
- Replay-Schutz
- eingeschränkte Datenfluss-Vertraulichkeit

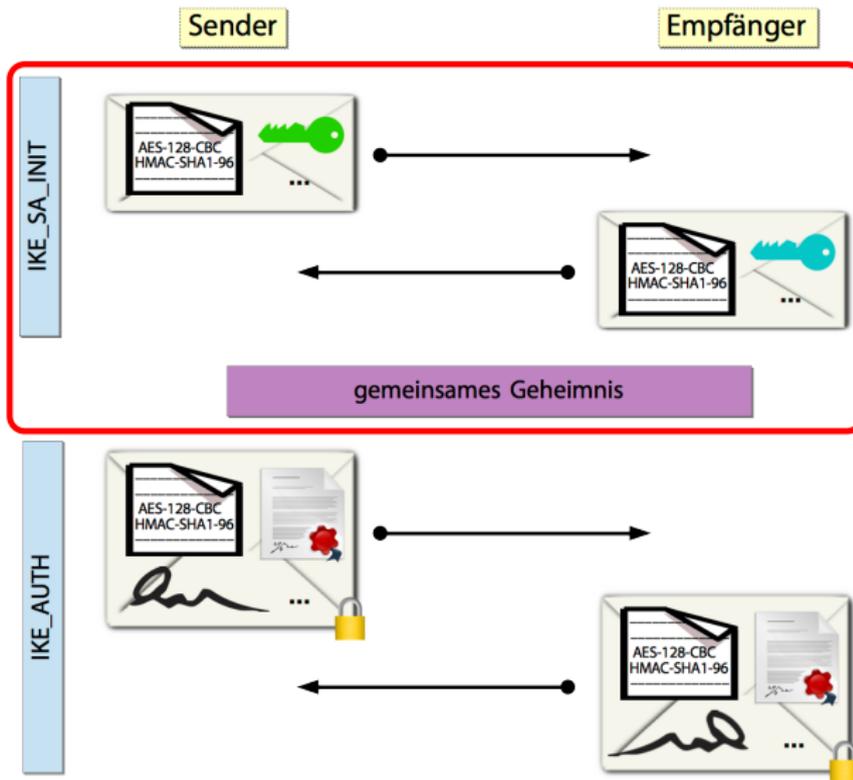


- Zugriffskontrolle
- Teilnehmerauthentifizierung
- verbindungslose Integrität
- Vertraulichkeit
- Replay-Schutz
- eingeschränkte Datenfluss-Vertraulichkeit

IKEv2 Protokoll - RFC5996



IKEv2 Protokoll - RFC5996





Geeignete Kryptosysteme für PQC



Geeignete Kryptosysteme für einen PQC-Schlüsselaustausch

- ~~Symmetrische Kryptographie~~
- ~~Hashbasierte Kryptographie~~
- Multivariate Kryptographie
- Gitterbasierte Kryptographie
- Codebasierte Kryptographie



Geeignete Kryptosysteme für einen PQC-Schlüsselaustausch

- ~~Symmetrische Kryptographie~~
- ~~Hashbasierte Kryptographie~~
- Multivariate Kryptographie
- Gitterbasierte Kryptographie
- **Codebasierte Kryptographie**

Codebasierte Kryptographie



- Fehlerkorrigierende Codes
- Verschlüsselung: Hinzufügen von Bitfehlern
- Entschlüsselung: Entfernen der Bitfehler durch die Kenntnis des Codes

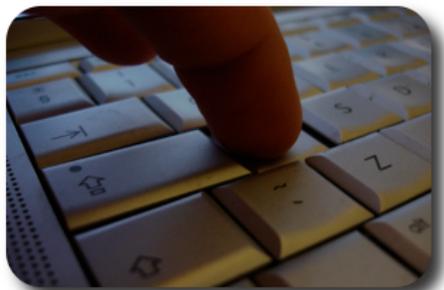
⇒ Vertreter: McEliece Kryptosystem, Niederreiter Kryptosystem

Codebasierte Kryptographie



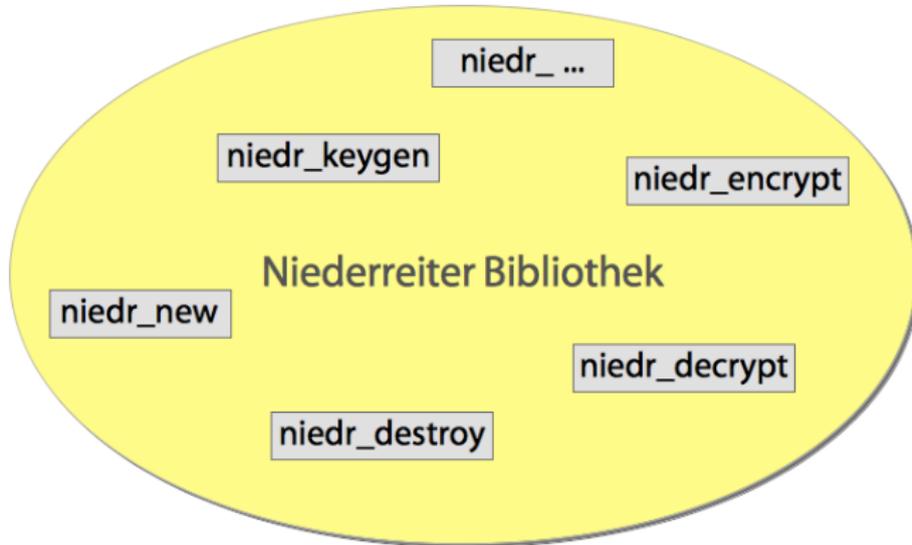
- Fehlerkorrigierende Codes
- Verschlüsselung: Hinzufügen von Bitfehlern
- Entschlüsselung: Entfernen der Bitfehler durch die Kenntnis des Codes

⇒ Vertreter: McEliece Kryptosystem, **Niederreiter Kryptosystem**



PQC-Implementierung

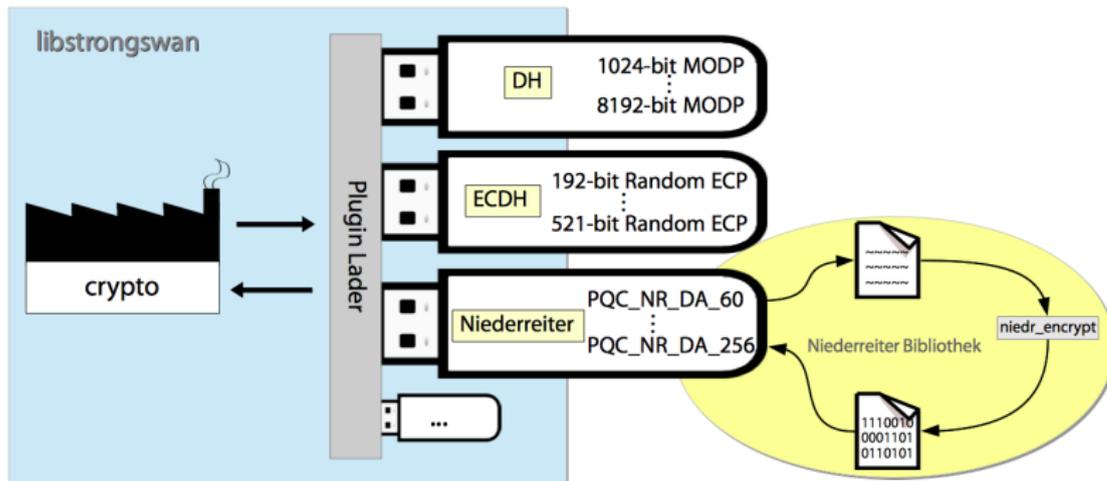
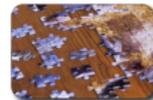
Niederreiter Kryptobibliothek



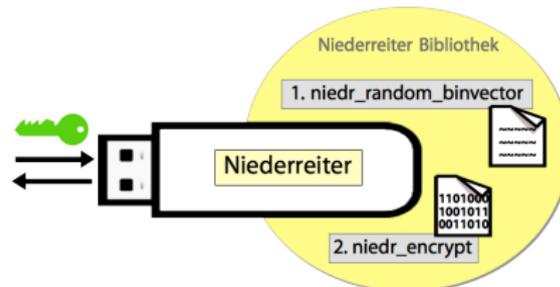
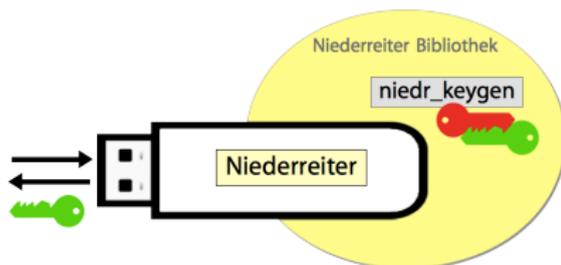
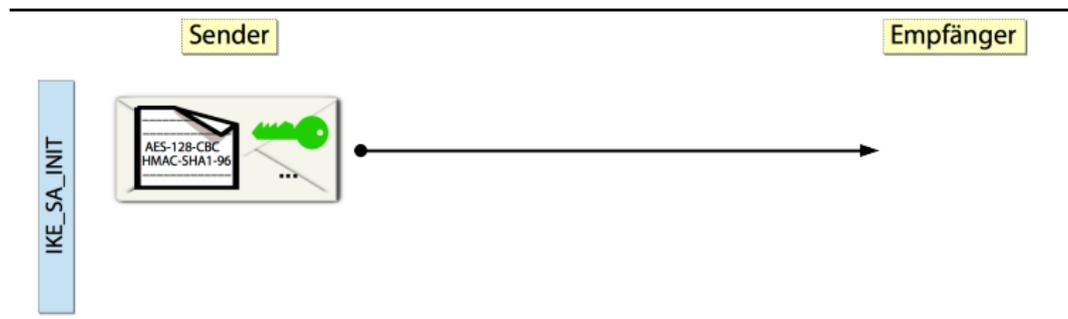
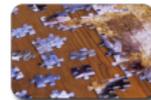


IPsec Erweiterung

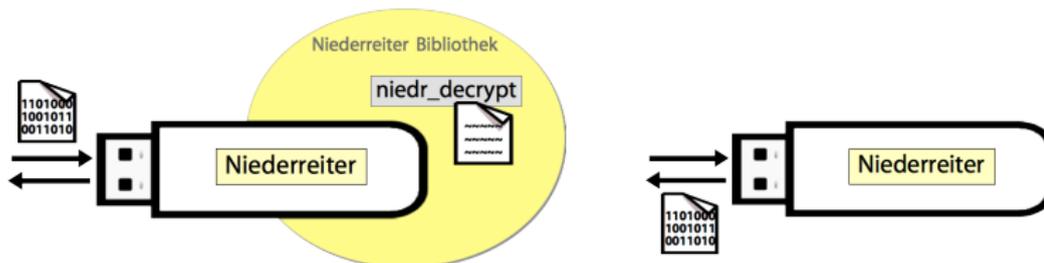
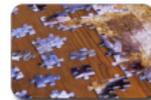
strongSwan Plugin



Erste IKE_SA_INIT Nachricht



Zweite IKE_SA_INIT Nachricht



Problem: Große öffentliche Schlüssel



Bit-Sicherheit	DH	ECDH	Niederreiter
128	384	64	443.088
200	1.024	-	1.097.560
256	-	132	1.924.824

Tabelle: Datenmenge in Byte für einen Schlüsselaustausch vom Sender zum Empfänger.

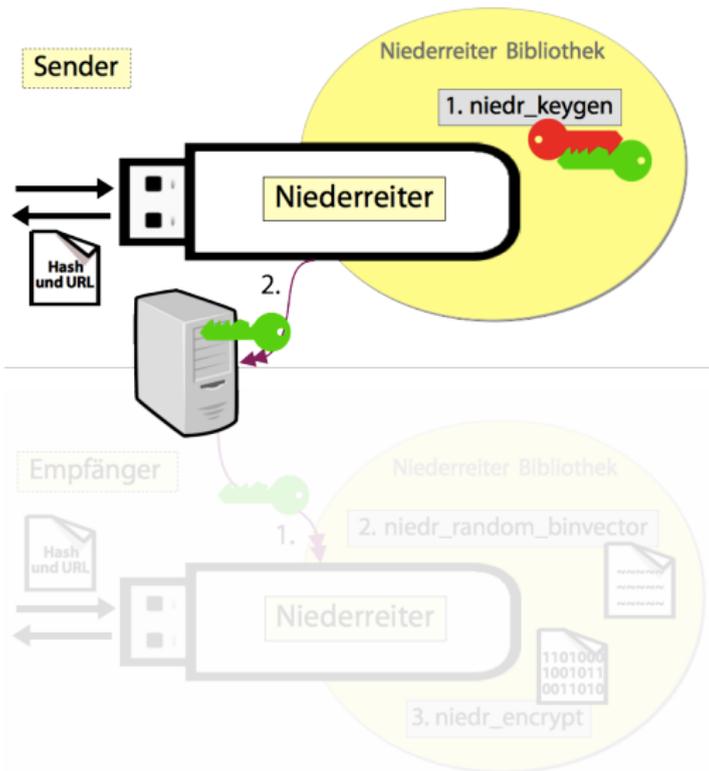
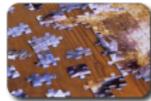
Lösung: Hash und URL



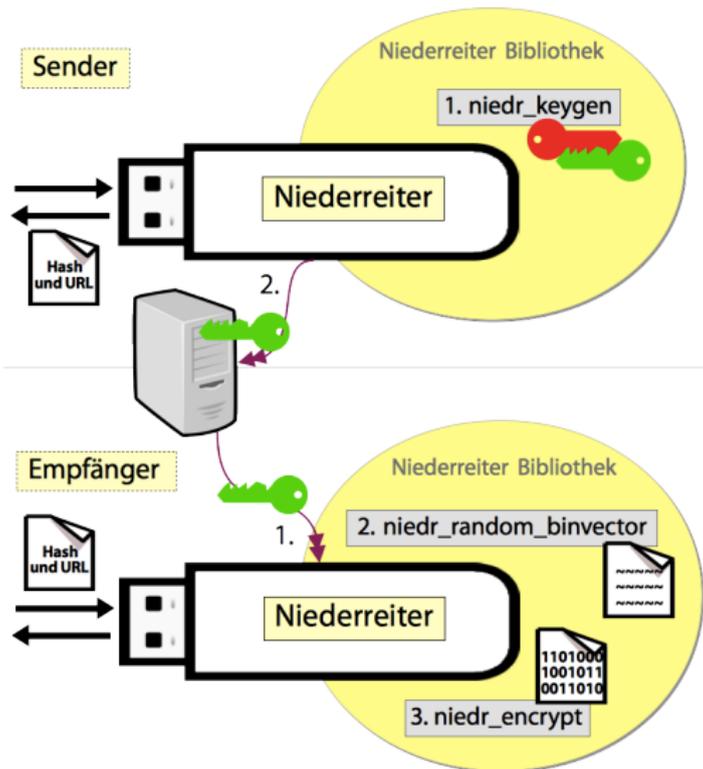
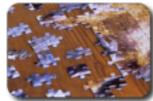
RFC5996

“by replacing long data structures with a 20-octet SHA-1 hash [...] of the replaced value followed by a variable-length URL that resolves to the [...] data structure itself.”

Lösung: Hash und URL

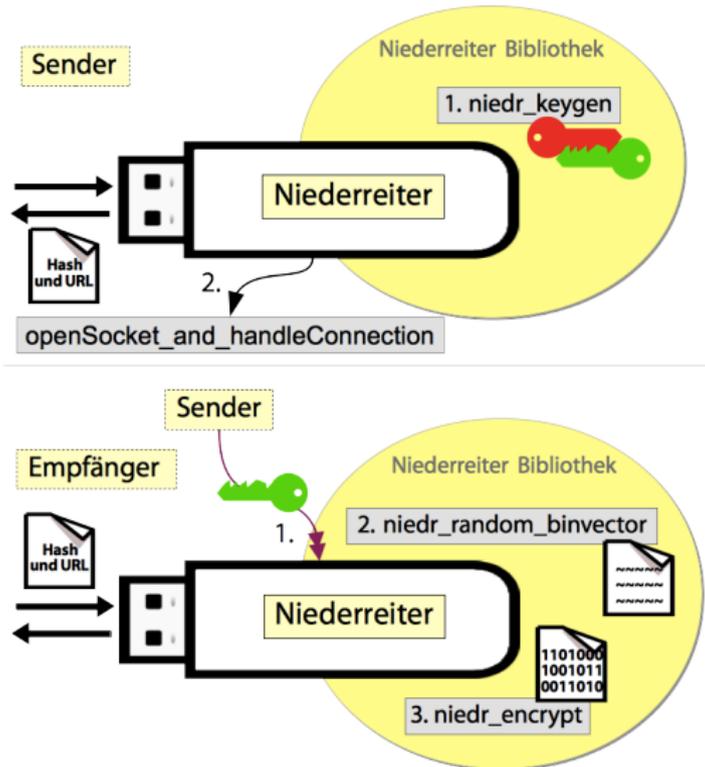


Lösung: Hash und URL





Lösung: Hash und URL mit Sendersocket



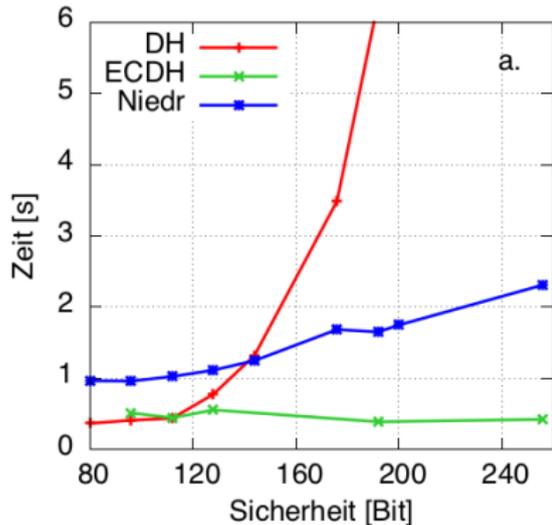


Evaluation und Vergleich

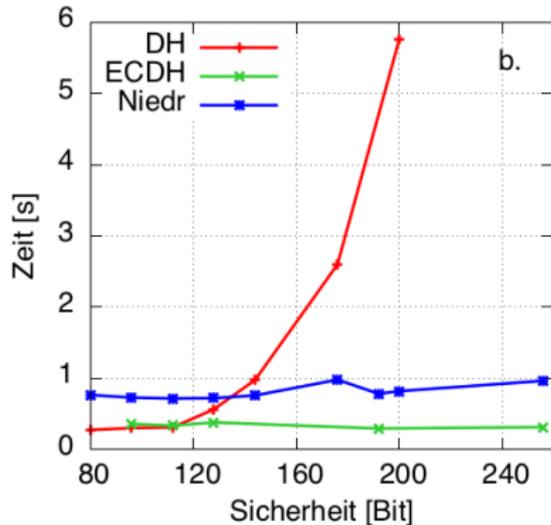
Latenz



Sender: IKE SA Aushandlung



Empfänger: IKE SA Aushandlung



Evaluation



- + Empfängerseite
- + Ver- und Entschlüsselung
- + Vergleich mit DH
- + Sicherheit gegen QC

- Schlüsselgenerierung
- Große Niederreiter-Schlüssel

Erreichte Ziele



- ✓ Ersetzung des DH-Schlüsselaustauschs mit PQC
- ✓ Erhaltung der Sicherheitsdienste von IPsec
- ✓ Keine Einführung neuer Angriffsmöglichkeiten
- ✓ Erste funktionierende PQC-IPsec-Verbindung

Lao Tzu

“If you do not change direction, you may end up where you are heading.”

- ▀▀▀▀ Verbesserung des Prototypen
- ▀▀▀▀ Einführung von PQC in kryptographische Standards
- ▀▀▀▀ Reduzierung der öffentlichen Niederreiter-Schlüssel
- ▀▀▀▀ Integration von PQC in IKE_AUTH





Analyse von IPsec und der notwendigen
Änderungen für PQC
→ Fokus auf *IKEv2*

Überblick geeigneter PQC Kandidaten für einen
Schlüsselaustausch

Prototypische **Implementierung** von PQC in IKEv2
→ *Niederreiter-Plugin* für strongSwan

Vergleich mit DH- und
ECDH-Schlüsselaustausch-Plugins und **Evaluation**

ezimmer@informatik.uni-hamburg.de

Backup-Folien

Wirklich noch keine Quantencomputer?

D:wave
The Quantum Computing Company™

HOME PRODUCTS & SUPPORT QUANTUM COMPUTING OUR STORY DEVELOPER PORTAL

Are you ready for this?

Applying our unique quantum computing technology, we aim to dramatically improve our customers' results through better understanding and insights.

Latest news > Quantum Computing Firm D-Wave Systems Announces Milestone of 100 U.S. Patents Granted - June 22, 2013

Quantum edge

Learn about how quantum computing provides a revolutionary new type of computational resource.

In the news

Press releases and news articles featuring D-Wave's products and technology

D-Wave Two

Integrated quantum computing system with 512 qubit chipset

Copyright 2012 D-Wave Systems Inc. All Rights Reserved | [Careers](#) | [Terms and Conditions](#) | [Contact](#)

http://www.dwavesys.com/en/dw_homepage.html » [5/5] Top

Was bewiesen werden konnte

- 1998: experimentelle Realisierung von Grovers Algorithmus für die Durchsuchung einer Liste von $N = 4$ Elementen nach einer speziellen Charakteristik [CGK98]
- 2001: experimentelle Realisierung von Shors Algorithmus für die Faktorisierung der Zahl 15 mithilfe von sieben Qubits [Van+01]
- 2011: experimentelle Realisierung von Shors Algorithmus für die Faktorisierung der Zahl 21 [Mar+12]
- 2013: effiziente Berechnung der Permanenten¹ einer quadratischen Matrix mithilfe eines nicht-universellen Quantencomputers [Til+13]

Auswirkung auf moderne Kryptographie

Schlüsselsuche	klassisch	Grover
Anz. Schritte für 128 Bit	$\frac{2^{128}}{2} = 2^{127}$	$\sqrt{\frac{2^{128}}{2}} = 2^{63,5}$
Anz. Schritte für 256 Bit	$\frac{2^{256}}{2} = 2^{255}$	$\sqrt{\frac{2^{256}}{2}} = 2^{127,5}$

Faktorisierung	klassisch	Shor
Anz. Schritte für 1024 Bit	$\approx 2^{90}$	$3,36 \cdot 10^7 [\approx 2^{25}]$
Anz. Schritte für 2048 Bit	$\approx 2^{117}$	$3,68 \cdot 10^8 [\approx 2^{28}]$

Tabelle: Durchschnittliche Anzahl an Rechenoperationen bei der Faktorisierung und der symmetrischen Schlüsselsuche.



Angreifermodell 1

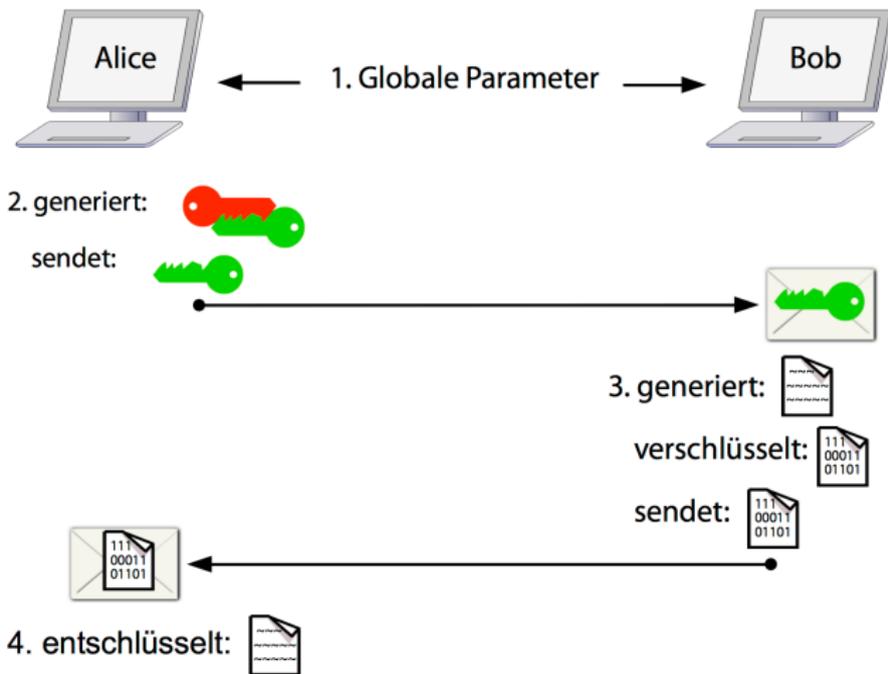
*Ein Angreifer habe die Rolle eines **Außenstehenden**.
Als dieser habe er nur Zugriff auf die Subsysteme zwischen den beiden
IPsec-Endgeräten der Kommunikationsteilnehmer, um durch IPsec
gesicherte Nachrichten abzufangen. Er verfügt allerdings nicht über
eine genügend große Verbreitung zur effektiven Unterbindung der
IPsec-Kommunikation.
Sein Verhalten sei als **aktiv und modifizierend** charakterisiert.
Die verfügbare Rechenkapazität und Zeit des Angreifers sei
komplexitätstheoretisch beschränkt.*



Angreifermodell 2

Ein Angreifer habe alle Rollen und Charakteristiken des Angreifermodells 1 und verfüge zusätzlich über einen Quantencomputer, auf dem er in Echtzeit Shors und Grovers Algorithmen ausführen kann.

Neuer IKE_SA_INIT PQC-Schlüsselaustausch





Niederreiter mit binären Goppa Codes

Code Parameter: $n, t \in \mathbb{N}$ mit $t \ll n$ als max. korrigierbare Fehler

Schlüsselgenerierung:

- Kontrollmatrix H_{priv} eines binären Goppa Code \mathcal{G}
- Zufällige Permutationsmatrix P
- Zufällige invertierbare Matrix M

$$\Rightarrow H_{pub} = M \cdot H_{priv} \cdot P$$



Niederreiter mit binären Goppa Codes

Code Parameter: $n, t \in \mathbb{N}$ mit $t \ll n$ als max. korrigierbare Fehler

Schlüsselgenerierung:

- Kontrollmatrix \mathbf{H}_{priv} eines binären Goppa Code \mathcal{G}
- Zufällige Permutationsmatrix \mathbf{P}
- Zufällige invertierbare Matrix \mathbf{M}

$$\Rightarrow \mathbf{H}_{pub} = \mathbf{M} \cdot \mathbf{H}_{priv} \cdot \mathbf{P}$$

- Öffentlicher Schlüssel: (\mathbf{H}_{pub}, t)
- Privater Schlüssel: $(\mathbf{M}, Dec_{\mathcal{G}}, \mathbf{P})$, mit $Dec_{\mathcal{G}}$ als Dekodierungsalgorithmus für \mathcal{G}



Niederreiter mit binären Goppa Codes

Verschlüsselung:

- Nachricht $\mathbf{m} \rightarrow \mathbf{e} \in \{0, 1\}^n$
mit Gewicht t
- Syndrom $\mathbf{s} = \mathbf{H}_{pub} \cdot \mathbf{e}$



Niederreiter mit binären Goppa Codes

Verschlüsselung:

- Nachricht $\mathbf{m} \rightarrow \mathbf{e} \in \{0, 1\}^n$
mit Gewicht t
- Syndrom $\mathbf{s} = \mathbf{H}_{pub} \cdot \mathbf{e}$

Entschlüsselung:

- $\mathbf{M}^{-1} \cdot \mathbf{s} = \mathbf{H}_{priv} \cdot \mathbf{P} \cdot \mathbf{e}$
- $Dec_{\mathcal{G}}(\mathbf{H}_{priv} \cdot \mathbf{P} \cdot \mathbf{e}) = \mathbf{P} \cdot \mathbf{e}$
- $\mathbf{P}^{-1} \cdot \mathbf{P} \cdot \mathbf{e} = \mathbf{e}$



Multivariate Kryptographie

- Basieren auf Mengen von quadratischen Polynomen $p_1, \dots, p_m \in \mathbb{K}[X_1, \dots, X_n]$ über endlichen Körpern mit mehr als einer Variablen
- Verschlüsselung: Auswertung der polynomiellen Abbildung am Nachrichtenpunkt
- Entschlüsselung: Anwendung der inversen polynomiellen Abbildung durch Kenntnis einer speziellen Abbildungsstruktur



Multivariate Kryptographie

- Basieren auf Mengen von quadratischen Polynomen $p_1, \dots, p_m \in \mathbb{K}[X_1, \dots, X_n]$ über endlichen Körpern mit mehr als einer Variablen
 - Verschlüsselung: Auswertung der polynomiellen Abbildung am Nachrichtenpunkt
 - Entschlüsselung: Anwendung der inversen polynomiellen Abbildung durch Kenntnis einer speziellen Abbildungsstruktur
-
- + Sehr effiziente Ver- und Entschlüsselung
 - + Frei für den kommerziellen Einsatz
 - Wenig Vertrauen durch viele gebrochene Kryptosysteme
 - Wenig Wissen durch Anwendung "junger" Mathematik



Multivariate Kryptographie

- Basieren auf Mengen von quadratischen Polynomen $p_1, \dots, p_m \in \mathbb{K}[X_1, \dots, X_n]$ über endlichen Körpern mit mehr als einer Variablen
 - Verschlüsselung: Auswertung der polynomiellen Abbildung am Nachrichtenpunkt
 - Entschlüsselung: Anwendung der inversen polynomiellen Abbildung durch Kenntnis einer speziellen Abbildungsstruktur
-
- + Sehr effiziente Ver- und Entschlüsselung
 - + Frei für den kommerziellen Einsatz
 - Wenig Vertrauen durch viele gebrochene Kryptosysteme
 - Wenig Wissen durch Anwendung "junger" Mathematik

⇒ Vertreter: HFE Kryptosystem, Perturbed Matsumotu-Imai Plus (PMI+)



Gitterbasierte Kryptographie

- Basieren auf Gitterproblemen wie dem Shortest-Vector-Problem oder dem Closest-Vector-Problem
- Verschlüsselung: Addition speziell präparierter Vektoren auf den Nachrichtenvektor
- Entschlüsselung: Invertierung der Addition durch Kenntnisse über die speziell präparierten Vektoren



Gitterbasierte Kryptographie

- Basieren auf Gitterproblemen wie dem Shortest-Vector-Problem oder dem Closest-Vector-Problem
 - Verschlüsselung: Addition speziell präparierter Vektoren auf den Nachrichtenvektor
 - Entschlüsselung: Invertierung der Addition durch Kenntnisse über die speziell präparierten Vektoren
-
- ± Starke Sicherheitsbeweise (dann allerdings nicht effizient)
 - ± Sehr effiziente Ver- und Entschlüsselung (dann allerdings keine starken Sicherheitsbeweise)
 - Wenig Vertrauen durch kurze Kryptoanalyse-Vergangenheit
 - Patentrechtliche Abhängigkeiten



Gitterbasierte Kryptographie

- Basieren auf Gitterproblemen wie dem Shortest-Vector-Problem oder dem Closest-Vector-Problem
 - Verschlüsselung: Addition speziell präparierter Vektoren auf den Nachrichtenvektor
 - Entschlüsselung: Invertierung der Addition durch Kenntnisse über die speziell präparierten Vektoren
-
- ± Starke Sicherheitsbeweise (dann allerdings nicht effizient)
 - ± Sehr effiziente Ver- und Entschlüsselung (dann allerdings keine starken Sicherheitsbeweise)
 - Wenig Vertrauen durch kurze Kryptoanalyse-Vergangenheit
 - Patentrechtliche Abhängigkeiten

⇒ Vertreter: Number Theory Research Unit (NTRU) Kryptosystem,
Learning with Errors (LWE) Kryptosystem

Gitterbasierte Kryptographie

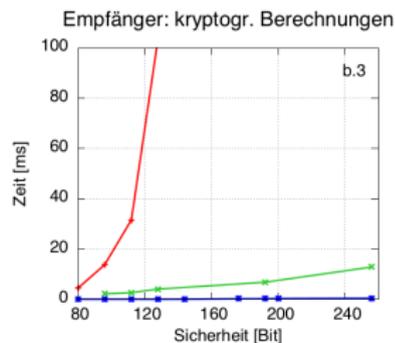
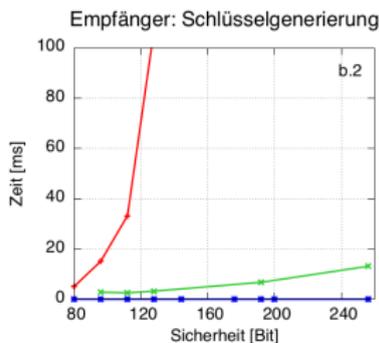
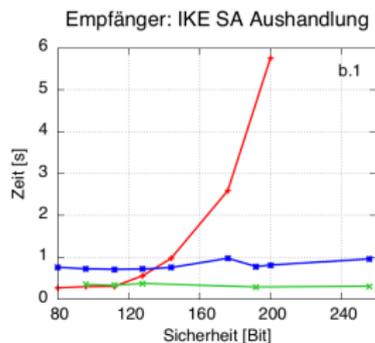
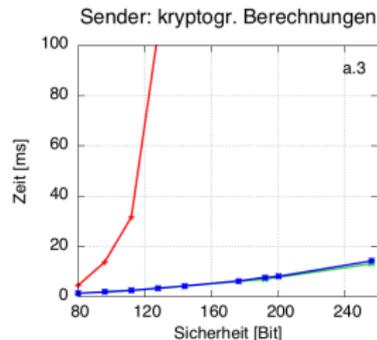
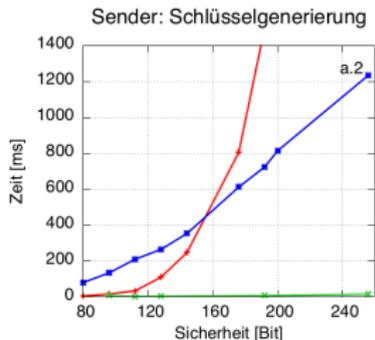
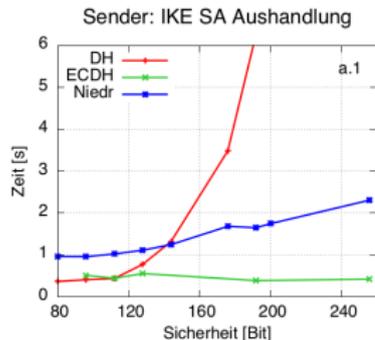


P. Campbell, M. Groves, D. Shepherd – 2014

“SOLILOQUY: A Cautionary Tale”. ETSI Crypto Workshop.



Evaluation: Latenzen





Latenz: IKE SA Aushandlung

Bit-Sicherheit	Sender [ms]			Empfänger [ms]		
	DH	ECDH	Niedr	DH	ECDH	Niedr
80	367,0	-	966,5	275,3	-	764,7
96	410,3	513,6	960,9	300,7	359,1	728,5
112	438,3	444,3	1.025,0	310,7	333,9	716,2
128	775,7	555,9	1.114,1	564,5	380,0	721,9
144	1.322,9	-	1.249,1	977,1	-	759,1
176	3.487,9	-	1.684,7	2.597,7	-	980,0
192	-	389,3	1.650,8	-	295,4	781,8
200	7.689,9	-	1.748,1	5.759,5	-	819,6
256	-	423,2	2.311,1	-	313,3	965,0

Tabelle: Zeiten für eine IKE SA Aushandlung mit den drei Plugins Niederreiter, DH und ECDH.



Latenz: Schlüsselgenerierung

Bit-Sicherheit	Sender [ms]			Empfänger [ms]		
	DH	ECDH	Niedr	DH	ECDH	Niedr
80	5,0	-	80,2	5,1	-	0,02
96	15,7	6,7	134,2	15,2	2,8	0,02
112	33,6	2,6	210,0	33,3	2,6	0,02
128	110,0	3,7	264,8	107,8	3,3	0,02
144	247,1	-	353,2	246,7	-	0,03
176	805,3	-	611,7	791,1	-	0,03
192	-	6,8	723,9	-	6,8	0,03
200	1.845,7	-	813,9	1.827,1	-	0,03
256	-	14,9	1.234,4	-	13,2	0,05

Tabelle: Zeiten für die Schlüsselgenerierung mit den drei Plugins Niederreiter, DH and ECDH.



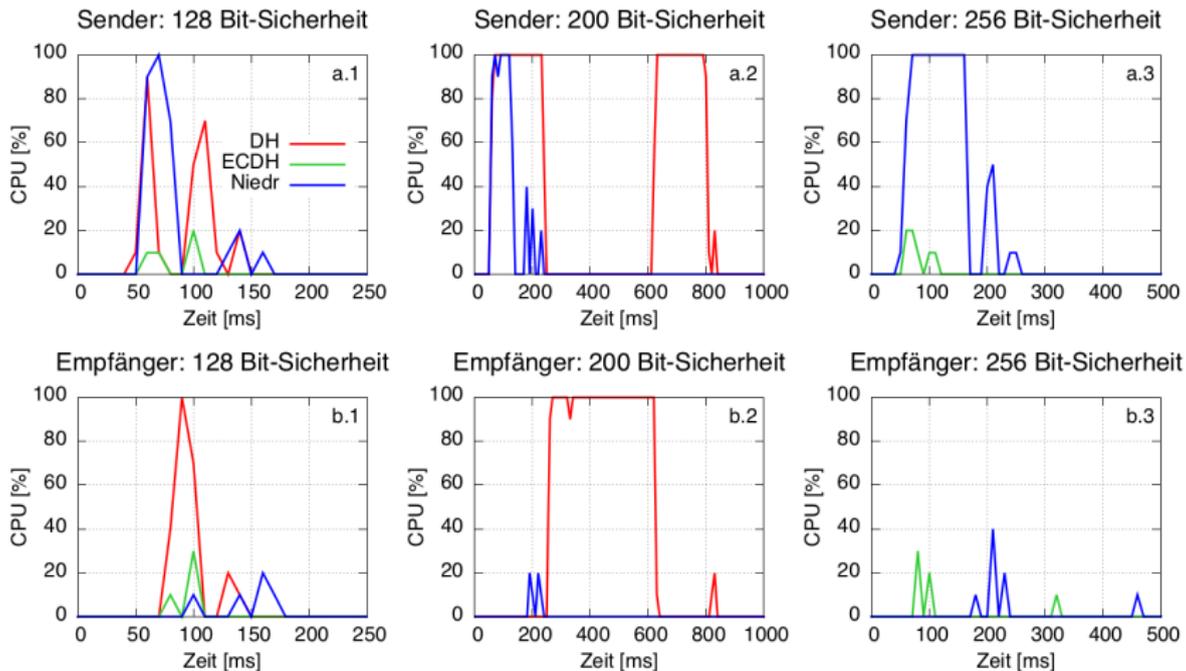
Latenz: kryptographische Berechnungen

Bit-Sicherheit	Sender [ms]			Empfänger [ms]		
	DH	ECDH	Niedr	DH	ECDH	Niedr
80	4,5	-	1,4	4,4	-	0,02
96	13,8	2,1	1,9	13,8	2,2	0,03
112	31,8	2,6	2,5	31,6	2,7	0,03
128	105,2	3,4	3,4	103,9	4,1	0,04
144	245,5	-	4,3	243,7	-	0,06
176	785,2	-	6,3	786,9	-	0,23
192	-	7,0	7,7	-	6,8	0,26
200	1.837,0	-	8,1	1.834,6	-	0,30
256	-	13,2	14,3	-	12,9	0,41

Tabelle: Zeiten für die kryptographischen Berechnungen mit den drei Plugins Niederreiter, DH and ECDH.



Evaluation: Rechenleistung



Referenzen I



Daniel J. Bernstein, Johannes Buchmann und Erik Dahmen. *Post Quantum Cryptography*. 1st. Berlin, Heidelberg: Springer-Verlag, 2009. isbn: 978-3-540-88701-0. doi: 10.1007/978-3-540-88702-7.



Isaac L. Chuang, Neil Gershenfeld und Mark Kubinec. „Experimental Implementation of Fast Quantum Searching“. In: *Phys. Rev. Lett.* 80 (15 Apr. 1998), S. 3408–3411. url: <http://link.aps.org/doi/10.1103/PhysRevLett.80.3408> (besucht am 15.07.2013) (siehe S. 37).



Lov K. Grover. „A fast quantum mechanical algorithm for database search“. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. STOC '96. Philadelphia, Pennsylvania, USA: ACM, 1996, S. 212–219. isbn: 0-89791-785-5. url: <http://doi.acm.org/10.1145/237814.237866> (besucht am 11.07.2013).



C. Kaufman u. a. *RFC5996 - Internet Key Exchange Protocol Version 2 (IKEv2)*. Sep. 2010. url: <https://tools.ietf.org/html/rfc5996> (besucht am 18.05.2013).



S. Kent und K. Seo. *RFC4301 - Security Architecture for the Internet Protocol*. Dez. 2005. url: <https://tools.ietf.org/html/rfc4301> (besucht am 18.06.2013).



Enrique Martin-Lopez u. a. „Experimental realization of Shor's quantum factoring algorithm using qubit recycling“. In: *Nature Photonics* 6 (Nov. 2012), S. 773–776. url: <http://dx.doi.org/10.1038/nphoton.2012.259> (besucht am 15.07.2013) (siehe S. 37).

Referenzen II



Peter W. Shor. „Algorithms for Quantum Computation: Discrete Logarithms and Factoring“. In: *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on Foundations of Computer Science*. Santa Fe, NM: IEEE Computer Society Press, Nov. 1994, S. 124–134. url: <http://dx.doi.org/10.1109/SFCS.1994.365700> (besucht am 10.09.2013).



Max Tillmann u. a. „Experimental boson sampling“. In: *Nat Photon* 7 (Juli 2013), S. 540–544. url: <http://dx.doi.org/10.1038/nphoton.2013.102> (besucht am 16.07.2013) (siehe S. 37).



Lieven M. K. Vandersypen u. a. „Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance“. In: *Nature* 414.quant-ph/0112176 (Dez. 2001), S. 883–887. url: <http://dx.doi.org/10.1038/414883a> (besucht am 15.07.2013) (siehe S. 37).